Final Degree Project

Grau en Enginyeria en Tecnologies Industrials

Perimeter Security 2.0

REPORT

Author:	Ignacio de Gregorio Noblejas
Director/s:	Juan Martín Jiménez
Speaker:	Manuel Moreno-Eguilaz
Call:	June 2016

Escola Tècnica Superior
d'Enginyeria Industrial de Barcelona

Resume

In essence, the basic objective of this project is to install and integrate a communication based perimeter security system that enables the company to manage and control these security devices from one unique point, effectively reducing costs and improving the solvency with which the company handles any possible security breaches.

Thereupon, the project has been thoroughly divided with the sole purpose of succeeding in the principle mentioned above. Initially a whole new network structure is set in order to assure that the perimeter security system that will benefit from it will work properly. To continue, the perimeter security structure is installed, and once this is done, it will be integrated onto the network structure. All devices will receive and IP address and the permissions to communicate with the programmable logic controllers and consequently with the monitor room that will be located in the headquarters and that will manage the whole security of the enterprise.

Conclusively, the company has evolved into a whole new level of security management and control, making it an up-to-date enterprise in that specific terms. Not only the company can solve complicated hazardous situations in an effective and comfortable way, but it can also do it whilst reducing the costs in terms of security personnel and facilities.

Summary

1. Glossary

Polybutadiene: Elastomer obtained from polymerization that is intended principally to the production of tires (approximately 70% of the world's production).

T_g: Glass-transition temperature is the temperature at which the polymer changes state from liquid to solid or vice-versa.

TCP/IP (*Transmission Control Protocol/Internet Protocol*): One of the foremost protocols found on Internet that is meant to create communication between machines to establish data flows.

Phishing: Basically, it's an impersonation of identity, in which the phisher pretends to be someone or a company to induce other people to grant them key personal information such as bank accounts or passwords from different social networks. Obviously it's considered an illegal act.

Fw (Firewall): Security at a communication level, it blocks any communication not permitted on an initial basis.

CTBA (Cuatro Torres Business Area): Financial district close to *Paseo de la* Castellana in Madrid.

Back-up: Copy of original data that is stored in order to have a way to recover information lost in case needed.

Hardware: All the physical parts in an informatics system.

Switch: Device whose utility is to interconnect two or more net segments, in a way very similar to net bridges, passing data from one segment to another using the destiny MAC address located in the network's frames and eliminating the connection once this one has ended.

Router: Device whose principal function consists in sending or routing data

packages from one net to another.

CCTV (Close TV circuit): As the proper name implies, it is a camera-monitor-cable closed circuit, which means it's not accessible from the exterior of the circuit.

UDP (User Datagram Protocol): Transport level protocol based in the exchange of datagrams. It is normally an alternative to TCP but without the need to establish a previous connection between machines, without flow control, provoking that packages may advance each other, and also without having confirmation that the package has arrived to its destiny. Due to this, its principal use consists in DHCP, BOOTP and DNS protocols (protocols in which is not worthwhile the usage of the TCP protocol) and also for audio and video streaming.

MJPEG (*Motion JPEG)*: Each photogram or field interlace of a digital video sequence it is compressed separately in a JPEG image.

MPEG4: Compression method for digital audio and video.

JPEG (Joint Photographic Experts Group): Compression and codification standard of fixed archives and images.

Doppler Effect: Discovered by the Austrian physicist Christian Andreas Doppler, it's the apparent change in frequency of a wave produced by the relative movement of the source from the perspective of the observer.

DMZ (Demilitarized zone): Secured net localized between the internal net and the external one of a company, being Internet the external one usually. The principal characteristic is that from the internal net it's permitted the access to the DMZ, but from this net it is not permitted the access to the internal net, but yes to the Internet.

PIR sensor (*Passive Infrared Sensor*): Electronic sensor that measure infrared lights radiated from objects in its field view.

CPD (*Centro de Procesamiento de Datos*, en ingles Data centre): Location where it's concentrated all the necessary resources needed for the processing of the information related to an organization.

Ethernet: Family of computer networking technologies commonly used in local area networks (LANs) and metropolitan area networks (MANs)

LAN (local area network): Computer network that interconnects within a limited area such as a residence, school, laboratory or office building.

MAN (metropolitan area network): Larger than a LAN, can cover up to few city blocks of an entire city.

Computer port: Serves as an interface between the computer and other computers or peripheral devices.

Web Browser: Software application for retrieving, presenting and traversing information resources on the World Wide Web.

World Wide Web: An information space where documents and other web resources are identified by URLs, interlinked by hypertext links, and can be accessed via the Internet.

URL (Uniform Resource Locator): Reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.

PLC (Programmable logic controller): Digital computer used for automation of typically industrial electromechanical processes, such as control of machinery on factory assembly lines, amusement rides or even light fixtures.

PTZ camera (Pan-tilt-zoom camera): Camera capable of remote directional and zoom control.

RJ-45 (modular connector): Electrical connector that was originally designed for its use in telephone wiring, but many applications include Ethernet jacks.

RFID (Radio-frequency identification): A device that uses electromagnetic fields to automatically identify and track tags attached to objects. These tags contain electronically stored information.

Slang: Lexicon of non-standard words and phrases in a given language (in this case English).

Epoxi resin: Thermostable polymer that hardens when blended with a catalyst meant to do so.

Magnetic induction: The production of an electromagnetic force or voltage across an electrical conductor due to its dynamic interaction with a magnetic field.

RS-232: Standard for serial communication transmission of data. It is commonly a standard computer port.

TTL: Technology based in a class of digital circuits built from bipolar junction transistors (BJT) and resistors. It has a standardized port for its use.

PIN (Personal Identification Number): Numeric password used to authenticate a user to a system, in particular in association with a credit card or an access card.

DNA (Deoxyribonucleic acid): Molecule that carries most of the genetic instructions used in the growth, development, functioning and reproduction of all known living organisms.

Smart card: Pocket-sized card that has integrated circuits embedded. (Credit cards for example).

State-space representation: Mathematical model of a physical system as a set of input, output and state variables related by first-order differential equations.

Model: Description of a system using mathematical concepts and language. They are usually composed of relationships and variables.

Feedback: Referring to control systems, feedback occurs when outputs of a system are routed back as inputs, forming a circuit or loop.

Relay: Electrically operated switch controlled by an electric circuit that, by means of a coil and an electromagnet, permits to open or close other independent circuits. Very commonly used to control other devices remotely using small control signs.

Panic Button: electronic device designed to assist in alerting somebody in emergency situations where a threat to persons or property exists.

Server Cluster: A cluster consists of two or more computers working together to provide a higher level of availability, reliability, and scalability than can be obtained by using a single computer. Microsoft cluster technologies guard against three specific types of failure:

- **Application and service failures,** which affect application software and essential services.
- **System and hardware failures,** which affect hardware components such as CPUs, drives, memory, network adapters, and power supplies.
- **Site failures in multisite organizations,** which can be caused by natural disasters, power outages, or connectivity outages.

DNS (Domain Name System): Hierarchical decentralized naming system for computers, services, or any resource connected to the Internet or a private network.

DHCP (Dynamic Host Configuration Protocol): Standardized network protocol used on IP networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

Directory Service: A service that organizes and stores the information regarding users from a computer network and the network resources that enables administrators manage the user's access to the resources of that specified network.

Domain: identification string that defines a realm of administrative autonomy, authority or control within the Internet. For example, "google.com".

IP address: numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.

Throughput (performance): Volume of lean flow information in a system, like a computing system.

Transport Layer: Provides the functional and procedural means of transferring variable-length data sequences from a source to a destination host via one or more networks, while maintaining the quality of service functions.

MacroLAN: A MacroLAN solution permits you to create private broadband networks using Ethernet ports with optic fibre, reaching velocities of up to 1000 Mbps.

2. Preface

In this preface I will explain briefly what is the main objective of this project. During these past years, the need of protecting and secure confidential information for a company has become key in order to preserve the wellness of the economy of that company. However, there has been several security breaches in very important corporations, such as *Sony* for example.

More often than not, big companies operating in more than one country have the need to control severely the security of their workers, especially in countries where the risk of kidnapping or thieving are seen continuously.

Consequently, the object of this project will be focused on perimeter security, physical, more than computer security, which will also be taken into account but in a more summarised manner.

2.1. Project Origin

Nowadays, the company *HidroPlastic S.A.* has the security managed in a decentralized manner, because the security of each location is managed in the same place. Each building has its own security employees, security centre and file server for data and records.

Moreover, this causes that there is no universal access. What this means is that if a worker or executive from Barcelona wants to travel to Madrid or Brazil and gain access to the buildings, his or her credentials will be denied for the security system, and the security workers will have to create an exception in order to let this worker go in. This is a far more expensive cost of time and money than it seems, and it also creates confusion and bureaucratic problems at all levels.

It is key to differentiate each case (Barcelona, Madrid and Rio de Janeiro) because each location has its own particularities.

Barcelona is the headquarters, and therefore it is where the majority of the confidential information is kept, as well as where the immense majority of important executive and meetings are held. Hence, in Barcelona the main objective of security management is to prevent as much as possible any possible information loss, not

only physically (archives and meeting listen outs), as well as digitally speaking (server hacking or personal computer hacking from high executives).

Consequently, in this case it is mandatory to control everything as much as possible, with strict access control, security camera utilization in all rooms where it may be considered helpful, fire sensors to prevent sabotage intents and also informatics security, with a particular department specialized in all types of cybernetic attacks, like aggressive port scans, phishing[1] and any possible activity considered as an attack by our experts, with the usage of firewalls[2] and installing antivirus in all our machines that need so, to prevent any vulnerabilities that could result in catastrophic consequences for our interests in protecting our information.

The case of Rio de Janeiro has particular characteristics. The fact that the factory is based on another country results in drastic legal changes that the company has to adapt to. In the case of Brazil laws are really different.

The greatest differences between Spain and Brazil are the legal references to workers. The Brazilian laws have big differences in comparison to the Spanish ones.

Worker' rights in Brazil are very protective against exploitation and discrimination:

- Trial period: It can be longer than ninety days. Also, work limitations can only last a maximum of two years, and in case the contract is renewed more than once, the company is obliged to contract the worker as undefined worker.
- Annual bonus: Any person that works in Brazil in a legal manner has the right to an annual bonus that is paid twice a year. What's more, extraordinary bonuses are paid 50% more and in festive days it can go up to 100%. Nocturne workers also receive bonuses from up to 20%, as well as works in which the health of the worker is in potential danger.
- Former notice of dismissal: It has to be done 30 days of more prior to the dismissal occurs. If it were the case that the worker had stipulated in its contract that he has to be notified before, the company is obliged to do so.

All these measures also apply to limited works and temporary ones (25 hours at a maximum), leaving out the last case in which extra hours are prohibited.

Besides, in Brazil the hour control is key and very strict, as workers are paid (due to the Brazilian laws) for worked hours.

In the last case, the case of Madrid will be very similar to Barcelona in terms of what the enterprise is interested in protecting, but with an important limitation. As mentioned before in the case of Madrid we hired a whole floor of a building to set an office. Therefore we can adjust and implant all the security we consider but always inside the perimeter of our floor. This means that we have no right to put perimeter security for the building or for other floors as they are not ours. This results in the fact that putting access barriers or other perimeter devices is useless.

Consequently, as we do not have full control of the security, we cannot assure our information is thoroughly protected, therefore key information will not be held there.

2.2. Existing solutions

The principal solution the market offers, which is the one we want to establish is to centralize all the organisation and management of the security of the company in one unique point, inside the headquarters, in the way we can monitor, control and organize the accesses, the storage of back-ups and also the persona information of workers, and prevent the enterprise from being susceptible to different disasters/attacks and at the same time succeed in complying the different laws related to this matter. For example, in the case of back-ups6[3], the government obliges every company to keep and store registers and data from workers, as well as security videos, in case the police needs them in an investigation. Apart from all this, we can also reduce costs in terms or hardware[4] as we do not have the need to establish servers in every location, we can control everything with the servers based on the monitor centre in the headquarters.

In the market, there exist different commercial products that can adapt perfectly to what we are looking for. As an introduction, we have IP cameras, IP fire sensors or practically any other security system one could think of, from pavement detectors to infrared barriers also with access to IP addressing. All these products will be properly addressed in chapter 4.

As a resume, technologies nowadays permit us to create communication between security devices, not only informatics devices but also perimeter devices. What's more, the security guard in control of the management of all this security net can also interact easily and successfully with these devices, ensuring everything works on plan and there is no area out of his/her control.

For example, IP cameras, these cameras have an Ethernet[5] port[6], to connect to the Internet by cable but also access to Wi-fi, to enable the personnel in charge of controlling these cameras the chance to view in real time from their computer or smartphone what the cameras are recording. This grants a margin to react to attacks with critical speed, and having a quick answer to unexpected events can improve the results dramatically.

2.3. Motivation

Considering the importance security is beginning to have in global companies, my motivation is to properly integrate a computer-communication based security system, that enables the company to manage and control security in a more efficient, operative and cheaper way, being up-to-date with the technology offered nowadays, to deter possible attacks from happening.

2.4. Previous Requirements

In order to go ahead and develop this project, not only I have had to apply all the knowledge I have acquired during my stay in Indra, but also had to dedicate full days (balancing my time with my duties at work) looking up information in the Internet and speaking to my co-workers and bosses in order to assure that what I am writing is true and corroborated.

Also, I have had to apply the knowledge I received doing the subject the university imparts named *Electrónica*, which was very nourishing and helped me a big deal when affronting this project.

3. Introduction

Nowadays there is not a single big company that does not use the globally well-known tool known as Internet. Not only the companies but practically all of us do on a daily basis.

Apart from that, any business that has something to hide from, public or any confidential information to keep in a safe environment has to guarantee the security tools to protect it anyway possible. Therefore the business has to have the necessary security devices, not only in a physical manner but also in a logical one (software and networks) going from user accreditation, access barriers and also servers that gather all the information needed and safes it for further use.

The company, whose name is *HidroPlastic,S.A.*, has developed a patent for a particular type of plastic very similar en terms of properties and looks, but not in composition (therefore it would not be considered different so it would not be a patent) to Polybutadiene[7]. However, it has a key difference when using these materials to create tires. The greatest advantage of Polybutadiene against the SBR (*S*tyrene-Butadiene Rubber) it is the glass-transition temperature T_g[8]. Having a smaller glass-transition temperature grants this new material a better resistance to abrasiveness and at the same time a low rolling resistance (the wheels do not slide). In other words, the endurance of the tires is a lot bigger. Consequently, if our new material has even lower glass-transition temperature, it will last far more than any other tire offered in the market.

What's more, one of the biggest problems Polybutadiene tires face is that it tends to slide pretty easily in wet surfaces, hence normally ends being blended with SBR to prevent this from happening, causing an increase in the final cost of each tire.

Consequently, one of the principal benefits the company's product offers is that it solves this sliding problem, therefore not needing any type of blend with other products, reducing costs not only of buying the raw materials, but it also facilitates the production, as you can produce tires with ease.

The company is divided into three locations:

1. Barcelona (headquarters): Central building.

2. Madrid (office): *HidroPlastic* has rented a whole floor in a building part of the financial district CTBA[9].
3. Río de Janeiro (factory): Factory destined to the production of the plastic.

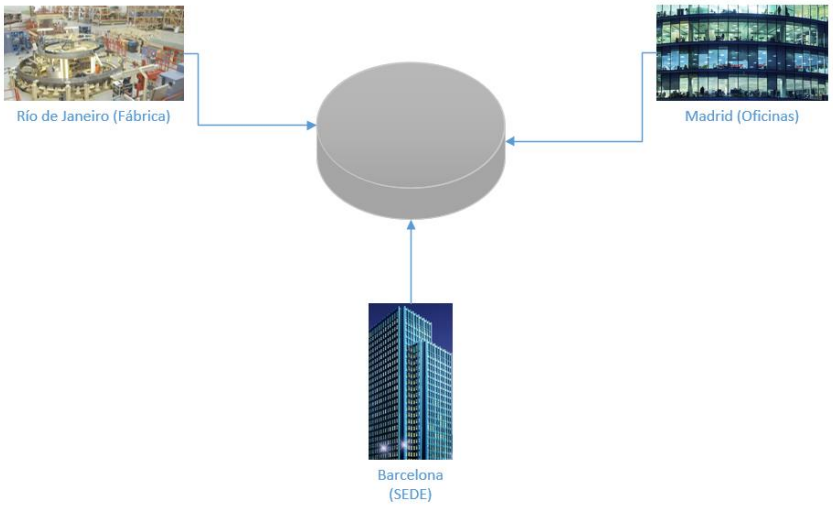

Figure 1 Company's Structure

3.1. Project's Objectives

The main objective of the final degree project is to establish the perimeter security system of a company with various locations, integrating a system that manages and controls all the sensors, access and exit control and other integrated electronic circuits using the communication infrastructure of the company, centralizing the service in the headquarters.

Using telecommunication protocols, especially TCP/IP and centralizing all the security in one unique point, we will provoke that all the security devices will communicate in an effective way and in real time between different locations, reducing costs significantly and facilitating the management of security, not only structurally but also legally.

To do so, apart from the installing of the perimeter security devices, it will be necessary to install all the necessary servers, such as DNS, DHCP, Domain Controller or File servers, as well as a proper own firewall and back-ups.

3.2. Project's Scope

The scope of the company consists of 3 locations: Barcelona (headquarters), Madrid (office) and Rio de Janeiro (factory).

Due to the fact one of the centres is located in a foreign country will provoke that we will need to take into account their laws and adapt to them.

4. Perimeter Security means which are available (physical)

In order to set the network infrastructure of the company properly, first we need to comprehend the devices that will benefit from this improvement.

4.1. Detailed description

In the case of *HidroPlastic,S.A.,* we are talking about a big and consolidated company, and due to the importance the high direction gives to this improve to the security management we want to approach, we will have all the necessary economical resources we need in order to succeed in our commitment.

Distinctly, neither of the locations will have the exact same perimeter security systems. For that reason, it is of utter necessity to approach each centre separately. Beforehand, however, we shall explain all the different security devices we are going to integrate in the system in a thorough way for best understanding further.

4.1.1. IP Cameras

An IP camera is a camera that has been designed specifically for sending recordings, images and even emails through the Internet by the use of a web browser[10] (Internet Explorer for example), as well as a through a switch[11] of a LAN[12] or MAN[13]. An example of the architecture of the net could be this one:

Figure 2. Camera Connection : DOMODESK

In the image we can observe how with just connecting our IP cameras to the router[14] installed in the network you can then communicate the IP Camera with the Internet and therefore anyone from external nets can gain access to the images recorded by that camera in real time if the user has de credentials to access not only the network, but also the IP camera.

The functioning is very simple. These cameras are composed of a traditional camera, an image compression system (to put these images in a format that can be sent to other devices for its proper visualisation) and also by a processing system in charge of managing the images and their sending. Also this processing system is in charge of controlling the movement of the camera and the detection system. To gain access to all of this you just need to connect the camera to a router but if the user want access just from the proper network the user will just need a switch and consequently this camera will have the possibility to communicate with all the other devices of the net.

The unique selling point of this product is that IP cameras can be accessed from any part of the world (this statement is sustained anywhere the user has access to Internet) and it can be applied to any situation possible: If the user has the camera installed in his/her home network he/she can access it from anywhere, his/her work or even the vacation location. If the camera is in a work network the security personnel can have visual access to areas they cannot see with their own eyes and as an extension any type of net imaginable, such as a hotel net, sport facilities, storage rooms, basements etc.

As a conclusion, any situation in which there is no other way to see what is going on if no camera is used.

What's more, IP cameras are not only designed for security usage. As an example, in the tourist industry it is common for hotels to install IP cameras for potential tourist to go to their web site and watch the installations or the views live.

Fundamentally, we need to see what IP cameras offer that serves as an advantage in comparison to the system the company uses in Madrid and Brazil, the CCTV[15]. The advantages are:

- World accessibility.

- Cheaper. IP cameras can be installed with ease, it is enough with connecting them to the router for them to become an element more in the network. Instead, CCTV circuits are expensive and hard to install.
- The network is absolutely expansible. You can add as many IP cameras as you wish (as long as the network is not saturated by excess of devices, or the PLC[16] cannot manage that much devices). In order to expand a CCTV circuit you have to duplicate the monitor during the expansion.

Figure 3. IP Camera and Ethernet Port. Tenvis (Amazon)

In the case of Madrid and Brazil, in which we use the CCTV system, integrate the IP system to the one initially installed is really simple, by using Video servers. This video server uses an analogic to digital converter and a compression and processing system to gain access to the Internet and consequently to the images recorded by the camera.

IP cameras can be manually controlled if needed, especially the ones called Pan-Tilt and Pan-Tilt Zoom *(*PTZ[17]*)*, (this last one if zoom is needed). More importantly, these cameras can be controlled remotely, by accessing them through Internet, previously identifying yourself with a user-password system.

A really striking feature these devices have is the possibility to integrate other sensors to the camera, such as fire sensors, movement sensors or smoke sensors. Either way the immense majority of IP cameras or video servers include a movement detection system, in order to detect, for example, if an object has entered

their field view and also they are able to differentiate if that object is alive or not.

Concerning the matter of exterior IP cameras, the producers have developed the necessary technologies to adapt the cameras to the changing weather. However, extreme it may seem, conditioning the camera to work efficiently in the most adverse weather conditions. For example, exterior cameras placed in the Brazilian factory will have to be extremely resistant to tropical climate and the extreme humidity.

One of the key factors concerning security is the access to the IP camera. In this case it is offered the possibility to establish several permission levels for users in order to administrate the camera, which are very similar to those of a conventional computer:

- Administrator: All permissions permitted. This means they have full control to administrate and change anything in the camera. In order to be administrator you need to the access the camera through an administrator portal, which requires identification with password by the user.
- User: They have permitted to view images and manage the camera (the guards and other security personnel in charge of controlling the day-to-day movements in the building. Also requires identification with a user and a password.
- Demo: Option offered by home automation companies that offers free access without identification. Obviously in our case this will not be permitted, as chances of suffering dangerous vulnerabilities for our security due to this are very high.

Apart from all the visual advantages the camera offers, it also disposes of high-sensitive microphones in order to transmit audio using de UDP[18] connection protocol.

Due to the fact that all these cameras are analogic, the video information is really high, and this is a problem because that amount of information cannot be transported by the cables of the network. In order to prevent this, the information has to be compressed somehow, losing as less information as possible in order to, despite the fact you are losing information, the information received is still sufficiently clear and useful to be used efficiently. Conclusively, these cameras dispose of two compressing systems, MJPEG and MPEG4, this last one the most recent and powerful. Any of these two compressors will permit us compress the information as much as possible not losing a single bit of key information.

When it comes to the visualisation of the images and for the visualisation of the administration portal, any web browser will be enough, for example *Microsoft Internet Explorer.*

At last but not least, in matters concerning the configuration of the IP camera, the first time you configure it you will need to connect the camera to a computer using a RJ-45[19]. However, once the camera has been configured once, the following times the administrator has the option to configure it remotely. At last but not least, as refers to the configuration of the IP camera, the first time that is configured it will have to be done directly connected to a PC by means of a "crossed" cable. Following that, it will be possible to configure the following set ups remotely.

4.1.1.1 Chosen Model

Probably, IP Cameras will be the most expensive of all devices, not for being the most expensive device by itself, but due to the fact the company will need a big quantity of them.

For that reason, the company has to find special offers that may decrease this price. The company needs both indoor and outdoor IP Cameras, as well as a switches (on to which we will connect the cameras before connecting them to the PLC. A provider named *VoipSUPPLY* offers a system formed by five indoor cameras and two outdoors as well as the switch for the price of 3600 dollars (3198.72 euros).

- Vivotek FD8134 (Indoor): Dome cameras (360º degrees). Works with MPEG-4 and MJPEG compression systems. Built in Infrared illuminators.
- Vivotek IP7361 (Outdoor): Day/Night, Infrared illuminators, SD card slot and works with MPEG-4/MJPEG compression systems.
- NetGear FS116P (Switch): 16 port switch to handle the seven devices.

Figure 4. IP Camera Pack. VOIPSupply

4.1.2. Detection sensors

Nowadays the market offers a great manifold of different movement sensors, for very variable utilisations, going from photoelectric sensors, ultrasonic sensors or proximity sensors. The applications are varied, they can be used for a factory, for example as a production line controller, for cases of fire or other types of emergencies and also it's very common their use for meteorological purposes. However, the most common use is to use them for security purposes, not only for preventing burglary or assault, but also as a health security system, especially on jobs in which the employee is at high risk of suffering severe injuries or even death.

Figure 5. Detection Sensors

4.1.2.1 Photoelectric sensors

Photoelectric sensors are sensors that utilize light beams to detect the presence or the absence of an object. These sensors are particularly effective when the object is not metallic (for example a human being).

- Background-suppression Sensor:

  Sensors specifically designed to ignore the background behind an object, be it clearer, darker or even the same colour as the object. In conventional sensors this situation could cause the sensor not to detect anything, and this is the reason this sensor is meant for.

Figure 6. Background-Suppression Sensor. Allen-Bradley

- Transparent objects detector:

  Sensors used for the detection of transparent materials such as clear glass, bottles and other transparent elements. Also used in the industry in general, due to the fact they have adaptable speed (as an example they can adapt to any production line speed).

Figure 7. Transparent objects detector. Allen-Bradley

- Optic fibre sensors

  Meant for detecting very small objects and verifying pieces in zones of difficult visual access.

Figure 8. Optic Fibre. Allen-Bradley

4.1.2.2 Ultrasonic sensors

They are sensors of a very advanced technology in comparison to the typical infrared sensor. Based on the emission of ultrasonic waves that outrange the human hearing range. Depending on the difference between the frequency of the emitted wave and the one received, the sensor will know if there is something in his emission scope that was not there before. As an added benefit, these sensors are capable of viewing or detecting through corners and objects and are capable of

detecting very small movements, and being able of reaching and control big areas.

As a result these sensors are great for offices, meeting rooms, long passages or lobbies. The principal problem these sensors show is that since they are very sensitive to slight movements, they can also react to object movements such as windows, doors, curtains or even papers moving during an impression.

There are two types of sensors, active and passive. The active ones emit signals and compare these signals with the received, whereas the passive sensors limit themselves to “listen” the emitted sound on a very wide range of frequencies. These passive sensors can be taught to being capable of distinguish certain particular frequencies like engines or air condition systems in order to not give false alarms for harmless situations.

Figure 9. UltraSonic. Allen-Bradley

4.1.2.3 Volumetric sensors

As the name itself describes perfectly, these sensors are built to detect the presence of voluminous objects such as people, animals or vehicles.

1. Infrared sensors

   Using the difference between the ambient temperature and that one of a human (for example), they capture the radiation generated by the intruder and the alarm goes off. The fact that they are so susceptible to weather

changes provokes that drastic changes in weather or in the air current in the building (due to the air conditioning) show chances of leading to false alarms.

Figure 10. IR Volumetric Sensor.ServiciosTC

2. Microwave sensors

These sensors are almost obsolete, due to being very prone to false alarms. They work based on the Doppler Effect[20]. The emissary emits a frequency that is reflected by the objects in its surroundings. In case of a variation of this frequency, this variation is captured by the receptor, which generates the alarm signal. Certain considerations or aspects have to be taken into account when installing these systems:

a. In case of installing more than one sensor, they have to be configured at different frequencies for them to not interfere between them.
b. Never install two equipment facing each other.
c. Never install these sensors facing windows, as the microwaves cross glass.

Figure 11. Microwave sensor. Intelbras

3. Mixed or double technology sensor

Sensor that unites both technologies explained above, infrared and microwave and that it only goes off when double detection occurs, both infrared and microwave, reducing this way all the possible false alarms for anomalous air currents or falling objects.
For its installation it has to be kept in mind the opening angle and scope, as well as the installing height, which normally is around two meters approximately.

Figure 12. Volumetric two sensor technology sensor. ServiciosTC

4. Outdoor volumetric sensor

   Detector very similar to those of the indoor ones with the slight difference that it disposes of a digital signal processor (DSP), apart from two PIR[21] channels with correlation technology in order to discard false alarms, such as home animals or drastic changes in temperature.

Figure 13. Exteriors volumetric Sensor. ServiciosTC

4.1.2.3.1 Chosen Volumetric Sensor Model

Obviously, now that we want to integrate this whole new perimeter security system, we want the best products (always at a logical price) offered by the industry.

OPTEX REDSCAN RLS-2020I: Indoor. Functionalities:

- Area allocation: You can specify particular areas in the room which want to be controlled (for example in an art gallery, only the paintings).
- IP protocol: UDP, TCP/IP and http browsing (to access the configuration interface)
- Capacity to link it to IP Cameras. If the sensor detects something moving in a particular area, the sensor can send an alarm to the camera that will immediately move towards the specified location.

Figure 14. OPTEX REDSCAN RLS-2020I. Optex

LC-171 (Outdoor Motion Sensor (Double PIR & Microwave, with Pet Immunity)

- Microcontroller signal processing
- Waterproof and temperature compensation
- Pet immunity up to 35 kg

Figure 15. LC-171. DSC

4.1.3. Barrier

Those centres that dispose of parking lots will have to dispose of access control barriers.

Concerning the different typologies of barriers that exist, they are normally divided into two groups, manual and automatic. Manual ones are thought for places of little transit, such as small parking lots, forest tracks or paths. Automatic barriers are meant for places with heavy transit, with flows of up to ten-thousand cars or vehicles in general a day.

4.1.3.1 Manual barriers

These barriers are quite simple in concept, since they have a manual action system in the barrier box. In most cases, the action is done with the insertion of a security key in the barrier box.

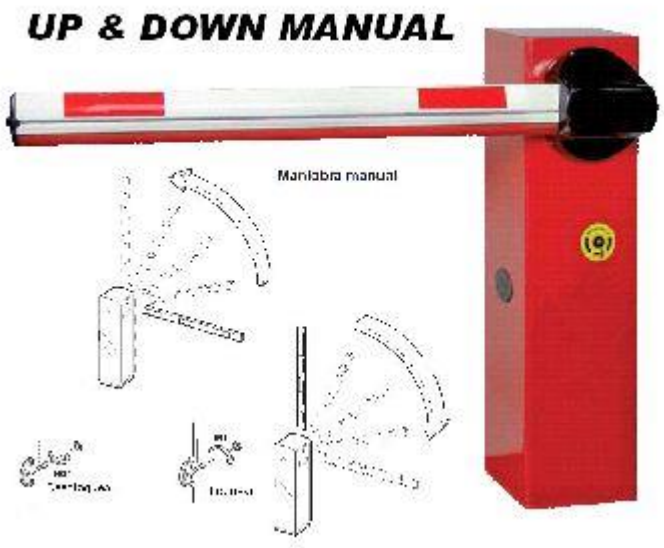

Figure 16. Manual Barrier. Accesor

4.1.3.2 Automatic Barriers

This type of barrier is far more complex, as they no longer need an operator that activates the barrier personally, but instead he/she activates the electrical controller or with automatic regulation. Some barriers activate themselves automatically

without the need of remote human control. Previously to lifting the barrier, it is common the usage of an identification system for the driver to identify himself/herself in order to access the building or centre. You can also configure the barrier to lift itself as soon as it detects the presence of a vehicle.

In the case of our company, it is very clear that the sole presence of a vehicle will not be enough to enter the building. If this was the case anyone could be capable of accessing the centre very easily. These barriers (presence detection barriers) are meant for other cases such as level crossings.

Apart from all of this, these devices can also adapt themselves to the present communication controls, such as the TCP/IP[22], as for example the case of *Night & Day Xtreme 68-ACR* of the *Accesor* company, that apart from having the chance to establish a communication protocol with her, it can manage approximately around 10000 times, whilst working under extreme conditions (the range goes from -30ºC to up to 60ºC).

4.1.3.3 Chosen Access Barrier Model

Ideally, we want a device that is automatic, to avoid the need to have a guard specifically in charge of controlling the barrier. Apart from that, we want the device to be adapted to TCP/IP protocols in order to make it manageable from a distance. For this reasons the company will use the model

Night & Day Xtreme 68-ACR:

- Up to ten-thousand maneuvers a day
- Five to Eight meters in length.
- High temperature working range (-30ºC up to 60ºC)

Figure 17. Night & Day Xtreme 68-ACR. Accesor

It is important to notice certain features the access control barrier must present, some included in the kit, others not. The kit includes a loop sensor on the floor to notice the cars or motorbikes and a photoelectric sensor to detect and prevent the barrier from hitting a vehicle.

Apart from the barrier, there is the need to buy an extra sensor to lock onto the barrier to act as the identification system.

4.1.4. Readers

In terms of control access, it is very important to have placed, in every entrance to every centre of our company, one or more proximity readers in order to fully control who accesses the building.

Adding to the fact of protecting the entrances to buildings, in some rooms, such as committee meeting rooms and similar cases, it is fully recommended to have an extra access control system. In rooms meant to store and protect data (like a data center[23]) this activity is also recommended.

The market offers various types of different access readers, going from card readers to fingerprint readers.

Although it will be explained thoroughly afterwards, this type of perimeter security will be key in Brazil because the laws there require it.

We can distinguish a range of different useful (for our case) readers:

- Proximity readers
- Magnetic Band
- Keyboard
- Biometric
- Receptor

4.1.4.1 Proximity readers

Proximity readers have obtained high levels of popularity these past years, reaching a point of being considered the industry standard for physical access control, due to its great liability and security in a very comfortable and easy way for the user.

The applications of these readers are varied:

- Access control
- Contactless Credit Card
- Electronic Wallet
- Digital signature
- Health Care Cards

Particularly, we will deepen in the case of the access control. Companies producing these readers offer different types of products, depending on the level of security needed. The typical reader is very similar to contactless cards, but are passive read-only devices. They contain an embedded RFID[24] antenna and can normally be read from distances from up to 10 feet (3,048 meters). RFID identifies objects by the means of radio waves. It works by employing a RFID tag and a reader. The RFID tag is formed by a microchip that has the information and an antenna that transmits the information to the reader and converts the radio waves into useful information.

Unlike bar-code systems and magnetic strike technology, RFID tag can be read anywhere inside the magnetic field sent out by the reader. Radio waves can be read through many metallic objects, and antennas can be embedded just about anything, like plastic cards and still be detected. Data is protected from environmental elements. Depending on the power of the reader, RFID antenna can read from direct contact up to 20 feet.

Some products of this type offer a second security level, often a keyboard in which you can safe number passwords that will be strictly linked to your card. These products offer you the possibility of just having access control with the card, only

with the password, or both.

Figure 18. Card-password reader. DSC

More often than not, these devices may incorporate an anti-vandalising system to detach intruders or whoever wants to break that system from doing so.

Chosen Proximity Reader

Suprema Xpass:

- IP/RFID
- Wiegand
- Optional access to PoE (Power over Ethernet)

Figure 19. Suprema Xpass. Suprema

4.1.4.2 Magnetic stripe card

Magnetic cards are capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material of the card. It is also commonly referred as swipe card or magstripe (slang[25]).

This magnetic band is present in a big variety of cards, such as credit cards, public transport control cards or personal cards. It is composed of several ferromagnetic particles embedded into a resin matrix (generally epoxi[26]) that store a certain amount of information with a certain codification that polarizes the particles.

Consequently, this magnetic band is passed through the reader and gets read by the means of magnetic induction[27]. In standard applications the information codified in these magnetic bands is organized in fields or tracks. The format and structure of these fields are regulated by the international standards ISO7813 (for tracks 1 and 2) and ISO4909 (for track 3).

The typology concerning these readers is very simple. They are divided into indoor and outdoor readers. Besides, something that tends to vary a lot is the connection port the reader uses (depending on where you want to connect the reader to). The common standards are RS-232[28] and TTL[29].

- Interior Reader:

Figure 20. DL03 Magnetic reader. Accesor

Ç

- Exterior Reader:

Figure 21. CLD123 Magnetic reader. Accesor

- RS-232:

Figure 22. RS-232. Misco

- TTL connection:

Figure 23. USB-to-TTL port connection. Digikey

4.1.4.3 Keyboard technology

Security keyboards are a brilliant and effective system of access control. In normal cases, this system is used at the same time as the card reader, as a form of adding another layer of security to the access control. Therefore, in terms of security it is not considered a sole security system of access control, but an additive to an already existing one in order to improve the security.

As shown above, many card readers nowadays incorporate this keyboard system, as the user who is trying to access the building, the room or whatever the system protects, he has to validate its card and also type the password on the keyboard. This password is directly and only linked to that card in particular, so passwords are unique and dependant on who is accessing. For that reason this passwords tend to be chosen by that user in particular, as any numeric password on any system nowadays.

On a regular basis, keyboards are used to enter the PIN[30], which consists of four digits, leading up to 10000 possible combinations. As I mentioned before, these keyboards are embedded onto normal access control card readers, to add an extra validation system:

Figure 24. Kaba card reader and keyboard. Kaba

Anyways, you can also just use the keyboard system like in this case:

Figure 25. Standard keyboard password Reader. Accesor

Chosen Keyboard Access Control

When seeking for the ideal Keypad the company needs a device that can resist impacts and hazardous weather conditions, as well as the obvious capacity to communicate with IP protocols.

Essex Electronics Keyless IP Series

- Works with DCHP or Static IP Networks
- Multi-Language
- Programmed via standard web browser (remotely)

Figure 26. Keyless IP Series. Essex Electronics

4.1.4.4 Biometric Readers

These are probably the most prestigious readers of all, and it is common their appearance in films as if they were the vanguard for access control technology. Biometry permits, with the use of automatized methods, recognise unique human parts of the body. They appear as a way to break from the traditional access control methods on which the concept bases on someone possessing (a key, card, etc.) or someone's knowledge (password, PIN, etc.). This type of access control can be seriously compromised, as it has plenty of security breaches that can be exploited.

Therefore, biometry is a very powerful technology, because it is not only capable of recognising human characteristics of the body, but also the behaviour. It can recognise almost every part imaginable, fingerprints, the human retina, DNA[31], the ear-form or even the veins on the hand and what's even more interesting, the body scent.

Hence, we need to establish a comparison between methods to decide which one suits the most. The principal methods include:

- Iris recognition
- Facial recognition
- Fingerprint recognition
- Hand Geometry

Iris recognition:

Iris recognition is nowadays the most common method of biometric access control readers. Not to be confused with retina scanning, it offers a great variety of characteristics:

1. Stable: The human pattern in the eye it's unique, lifelong and is formed from 10 months old onwards.
2. Unique: Chances of two people with same pattern is close to none. Experts suggest the chances are around 1 in 10^{78}.
3. Flexible: Easily adapted to any security installed, very easy to integrate.
4. Reliable: Grants great access control protection.
5. Non-invasive: Unlike retina scanning, it's contactless and harmless.

Advantages of iris recognition:

- Almost everyone can have access to this technology, even blind people, as it is an iris-dependant technology, not sight-dependent.
- Iris pattern is unique and lifelong. Only in cases of trauma, eye surgery or similar situations can make someone's iris pattern change, so once someone is registered in the device, seldom will he/she need to update the pattern.
- Iris recognition is the only technology that is designed to work in the 1-n or exhaustive search method. This is ideal to manage and control large databases such as the National Documentation application. Like any other method worldwide, it is not perfect, as has always a chance of failure. However, it performs in a really effective way when working with large databases.
- Up to 20 times quicker than any other known technology.
- Safety and Security Measures in Place. Iris recognition involves nothing more than taking a digital picture of the iris pattern (from video), and recreating an encrypted digital template of that pattern. 512-byte iris templates are encrypted and cannot be re-engineered or reconstituted to produce any sort of visual image. Iris recognition therefore affords high level defence against identity theft, a rapidly growing crime. The imaging process involves no lasers or bright lights and authentication is essentially non-contact.
- Very intuitive interface and use.

Disadvantages of iris recognition:

- A lot of memory to be stored.
- Very expensive
- Some older systems have been proofed to be intrusive.

Figure 27. Iris recognition. Serban Biometrics

Facial recognition:

During the past several years, face recognition technology has received significant attention for its variety of applications, both law enforcement and non-law enforcement.

One of the greatest advantages of facial recognition is that is a non-contact process, therefore physical interaction between the user and the system is never demanded. Besides, the images (the system works by taken a photograph of the person) can be stored easily for future interactions.

In terms of advantages of this system, they are as follows:

- No more time fraud. As al workers have to go through the facial recognition system to check in (for example), nobody can fool the company pretending they are working when they are not, as the facial recognition system will store his/her face in case he does check in.
- Better security. You can track everyone who has entered the facility, as you have his/her face stored in the file-server. So in case of a security breach, you have almost for sure the burglar's face in you database.
- Automated Facial System. This systems do not need to be monitored 24/7, they are meant to work in an automated way.
- Easily Integrated. These systems can be integrated into your system very easily, eve working with software already existing in your system, as they are very adaptable in this matter.
- High success rate. Due to modern day 3D face recognition technologies, it is very hard to fool this system.

Disadvantages of facial recognition

- In case the system works with 2D technology, the recognition can be influenced by lighting, person's hair, age, and even if the person wears glasses.
- Up until almost all PCs include cameras, the technology is susceptible of not becoming popular.
- Privacy concerns: People do not know when their image is being taken and what's worse, stored in a database. These images could be used without explicit permission from the person.
- Secondary processing is sometimes required, especially in surveillance operations.

Figure 28. Facial Recognition. Tech-Faq

Fingerprint recognition:

Automated method of identifying or confirming the identity of an individual based on the comparison of two fingerprints. Not only is fingerprint recognition one of the most known biometric access control security methods, but also by far the most used one (with iris recognition), and probably the main reasons for this to be like this is the fact that it can acquired with ease and a technology widely accepted. Besides, this technology can be used at a maximum of ten times per person (ten fingers).

Firstly, we will look into detail what the basic patterns in a fingerprint are, these are the arch, the loop and the whorl:

- Arch: Pattern where the ridge enters one side of the finger, then rises in the centre forming an arch, and exits on the other side of the finger.

Figure 29. Arch Pattern. Biometric-Solutions.com

- Loop: The ridge enters one of side of the finger, forming consequently a curve and then exits the finger on the same side it initially entered.

Figure 30. Loop Pattern. Biometric-Solutions.com

- Whorl: Pattern that occurs when ridges circle around a central point.

Figure 31. Whorl Pattern. Biometric-Solutions.com

However, these are only the main patterns in a normal fingerprint that can be found in humans. In spite this fact, fingerprints are unique to each individual, and this is due to small features or minor details that can only be found in one fingerprint, bringing that fingerprint apart from all the others. These minor details that differ between fingerprints are the ridge ending, the bifurcation between two different ridges and spots, ridges that are significantly smaller than other ridges. The main advantages of fingerprint recognition are as follows:

- Universality: Very few people will miss all 10 fingers, it is a very rare condition. The majority of fingerprint recognition software offers the possibility to store multiple fingers per human being in case of an injury occurring.
- Uniqueness: Fingerprints are proofed to be unique to each individual. Although there is always a chance of two fingerprints being the same, this chance is not hazardous at all, as the possibility is remote at the very least.
- Permanence: Fingerprints do not change is we grow older. However, the loss of collagen by older people could induce the system to more false recognitions. Despite this, storing multiple fingerprints per person reduces the likelihood of the system failing.
- Collectability: Very easy to acquire, these systems, even the most effective and efficient, are not very expensive, making them very accessible at a medium-low cost.
- Acceptability: Very accepted by users as fingerprints do not give sensitive information about yourself, such as medical conditions.
- Circumvention: There has been many cases of people cutting off their fingerprint or using dummies or photocopies. However this fraud can be solved using human activity detectors embedded into the system. These detector will notice if the object is not alive, making it very hard to fool the system.
- Performance: Performs generally really well at almost any level of demand.

Disadvantages of fingerprint recognition:

- For some people it is very intrusive and uncomfortable, as they related it to criminal identification.
- Not appropriate at young ages, as kids are susceptible to changes on the fingerprint.
- Fingerprint recognition is not as accurate as iris recognition. Fingerprint fails 1 in 100000 statistically speaking, whereas iris fails around 1 in 1.2 million.
- Fingerprint systems measure around 60 characteristics to differentiate each finger, whilst iris recognition up to 240.
- As the system requires contact, the hardware has to be kept clean.

Figure 32. Fingerprint Recognition. Wikipedia.org

Hand Geometry:

Hand geometry was the very first biometric recognition system ever, making its debut in the late 1980's. For that reason, adding up to the fact it is very easy to use, makes it a very widely accepted and used method.

As mentioned above, it was the first system implemented, debuting in the market in 1986, patented and developed by David Sidlauskas. The first major even that used this system was the 1996 Olympic Games.

How does the system work? The concept is very simple. Just by means of measuring the length, width, thickness and surface area of an individual's hand while guided on a solid surface. Then, the system uses a camera to generate and capture a silhouette image of the hand.

Figure 33. Hand placed in the surface. Biometrics.gov

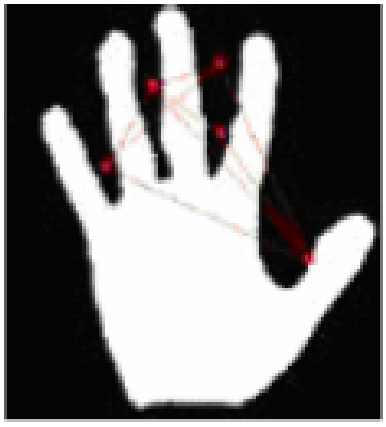

Figure 34. Generated silhouette of the Hand. Biometrics.gov

In total, the system goes taking images of different perspectives of the hand, analysing up to 31000 points and takes up to 90 measurements. These measurements range from the length of the fingers, the height, the thickness or even the distance between knuckles.

The advantages concerning this system are the following:

- Information can be stored in nine bytes of data, a very low number compared to other biometric systems.
- Although requiring special hardware, it is very easy to integrate into other devices or systems.
- Very accepted nowadays, as it is foreseen and accepted as a common access control system.
- As it requires little data, it can be used with Smart Cards[32] easily.

Disadvantages regarding hand geometry:

- Very expensive, especially concerning hardware.
- Considerable size.
- Not valid for arthritic people, as they cannot be scanned properly.
- Hand size can be affected by weather conditions, illnesses or even pregnancy.
- Some people may be reluctant to put the hand where many have already, provoking a hygiene issue.

Figure 35. Hand geometry System. Biometrics.gov

In order to simplify costs and facilitate the integration of biometric systems in our company, we need to decide which of the biometric access control systems suits the company in terms of security, reliability, devices required (regarding the integration) and price, among other characteristics to be taken into account. According to many biometric web-sites, the comparison can be resumed like this.

Biometric Technology	Accuracy	Cost	Devices Required	Social Acceptability
Iris Recognition	High	High	Camera	Medium-low
Facial Recognition	Medium-low	Medium	Camera	High
Hand Geometry	Medium-low	Low	Scanner	High
Fingerprint Recognition	High	Medium	Scanner	Medium

From this perspective, it is very clear that our choice will be fingerprint recognition, as it has high accuracy, is cheaper than iris recognition and somehow more accepted socially than this technology. Besides, we will look for a product that supports standard communication protocols such as TCP/IP.

Figure 36. Fingerprint Reader with TCP/IP option

Chosen fingerprint model

Considering this particular type of devices, the company wants the best there is out in the market. This technology will only be used in very specific places, guarding the most important technology. Therefore *HidroPlastic S.A.* considers that the investment can be bigger in this case to ensure the security is improved. Therefore, one of the vanguard companies in terms of biometric systems is *Suprema*.

Suprema BioEntry Plus

- Works with TCP/IP
- Operating Temperature -20ºC to 50ºC
- Multi-Controller
- 2 Internal Inputs and 1 internal relay output to control peripheral devices
- Chosen best fingerprint device in FVC 2004,2006 / NIST (National Insitute of Standards and Technology) MINEX 2008

Figure 37. BioEntry Plus. Suprema Inc.

4.1.5. Photocells and perimeter towers

Photocells are light-controlled variable resistors. This resistance of a photocell decreases with increasing incident light intensity. Using a turret in order to protect the photocell, we will generate a sort of infrared wall surrounding the buildings to prevent unexpected entrances. As it is a very restrictive perimeter security device, these photocells will only work at night and weekends. Using them during the day will only make the alarm go off every now and then, which would be a waste of resources and particularly annoying for workers due to the sound, and especially for security workers for wasting their time.

The device itself consists of two main parts, the photocell itself and the housing that protects it from outdoor effects. Therefore, the devices that will be used for this purpose will be:

Figure 38. EPCOM ABT100L (2 beams, 30m-100m). Epcom

This beam will be located inside a turret specifically meant for that usage, and these turrets will be located in the outdoors of the perimeter of the building, ideally in the verges of it.

Figure 39. Perimeter one-face turret for photocells. Epcom

Figure 40. Photocell turrets working. Epcom

Chosen photoelectric perimeter security sensor

Optex AX-200TN

- Anti-frost hood cover
- Anti-vandalised system
- Indoor/Outdoor
- Up to 200ft (approximately 61 meters)

Figure 41. AX-200TN. Optex 1

4.2. PLCs in automatic control

Up until now everything that has been covered up has been related to the main theme of this project, integrating a communication-based perimeter security system in order to control everything in real time and from one unique point, but all this will not be possible unless programmable logic controllers[33] are used.

However, before setting ourselves of talking through programmable logic controllers, we need to understand that these controllers work in a bigger control system.

4.2.1. Control systems

A control system is a device, or set of devices that manages, commands, directs or regulates the behaviour of other devices or systems. We can clearly differentiate two types of control systems.

4.2.2. Open-loop control system

Also called non-feedback controller, it is a type of controller that computes its input into a system using only the current state[34] and its model[35] of the system.

The principal characteristic of open-loop controllers is that they do not use feedback[36] to determine if their output has achieved the desired goal of the input. This means that these systems cannot correct errors.

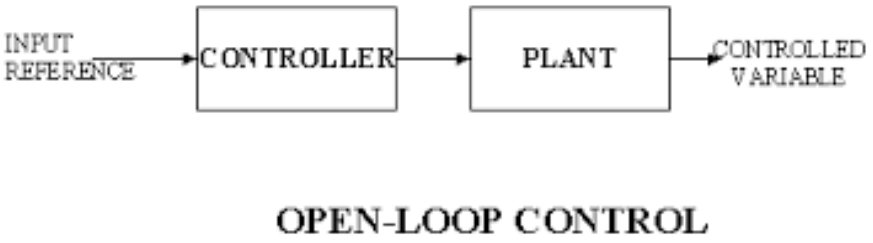

Figure 42. Control Diagram. Wikipedia.org

4.2.3. Closed-loop control system

It is a similar concept as the open-loop but with the additive of a feedback that controls the states or outputs of a dynamical system. In order to assure actions are being controlled properly, this method will be used to manage the security systems.

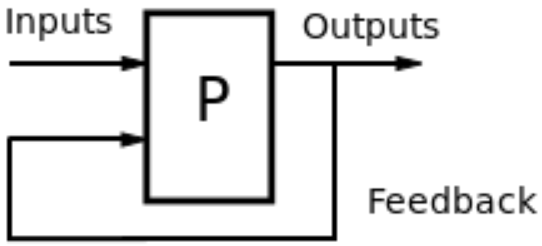

Figure 43. Control Diagram. Wikipedia.org

4.3. Controller

These control systems use sensors, actuators, controllers and other devices to function, and in our case that controller will be a Programmable Logic Controller or PLC[37].

Programmable Logic Controllers are a key part in this project, since these computers are in charge of controlling the security devices. Each controller can manage up to 16 different devices.

4.3.1. How Programmable Logic Controllers work

A PLC is a very simple concept. It basically consists of input and output terminals, a port for the programming cable a digital to analogic card and an analogic to digital card as parts of the hardware and the software to create the programs that will manage the PLC.

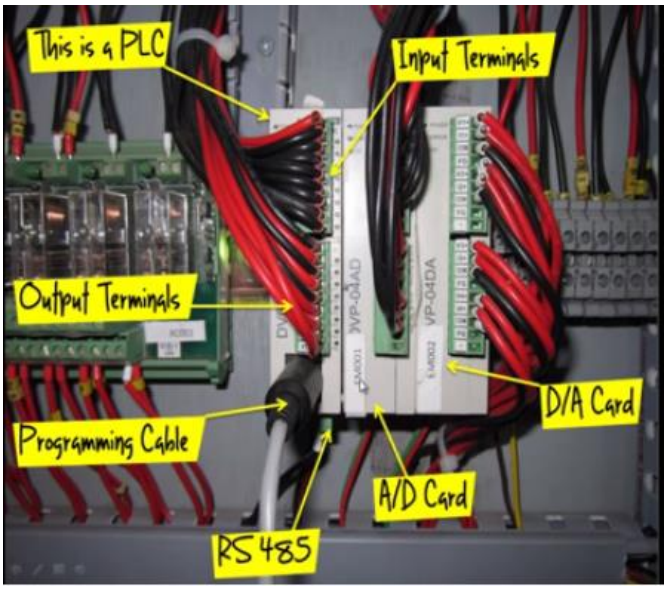

Figure 44. Programmable Logic Controller. Youtube.com

For example, with one unique controller the security department can manage up to 16 different devices, each one with its unique software and management.

In many ways, programmable logic controllers are indeed computers. Like any other computer, they dispose of non-volatile memory, to store the software, previously designed in a special application in a computer and using the programming cable consequently stored in the PLC.

They work as follows:

The company installs a device in a particular room. When the camera is configured, the installer gives the order to set the alarm off when something moves in that room. Once the camera is configured, it has to be linked onto the programmable logic controller. This controller has previously been installed a software to manage the inputs received by the camera.

Basically, if the camera notices something moving that should not be, it will be registered and consequently the camera will send an alarm to the controller. This signal will be received by the controller that will act conclusively. For example, if the company wants to shut all exits to the room if a camera notices movement, it is the controller the device that does that action.

In the case of this project the company needs controllers that can manage as many devices as possible, to reduce costs. Moreover, these controllers need to have the option to be extended and located in buses of many controllers to enable the security department to manage the whole facility with ease.

Chosen Programmable Logic Controller

Consequently, the DS216 from the company *Accesor* will be explained thoroughly. This device can manage up to 16 digital supervised inputs and 4 relays[38]. This capability can be extended up to twenty-four inputs by adding an extra plug-in extension board and sixty-four relays by the use of another type of extension board. In order to manage more devices, another controller shall be installed. In the case of this controller, alarm events can be transferred not only by cable (RS485 standard use) but also by TCP/IP, which is the key to the company's interest. Each input can be supervised separately, as well as the status of the line.

These devices when ordered usually come with their own specific software. In this case, this software is called *Amadeus 5*. Using this software you can define the behaviour of the system as:

- Inputs physical status: "Normally open" or "Normally closed".
- Input state: "Armed" or "Disarmed", either manually or according to time zones.
- Reflexes: Activation of one or several relays upon detection of specific input(s) status.

One of the principal stand-outs this controller offers is that it can register and record up to 4500 alarm events in its internal memory.

Figure 45. DS216. Accesor

5. Proposed solution

Once all the key devices have been thoroughly explained in the previous chapter, it is time to explain in detail what the proposed solution is. As explained in the opening chapters, the main objective of this project is:

Until now, in *HidroPlastic S.A.* all the management of security has been done in a decentralized manner, which means every location had its own security room with its own video wall and servers, as well as security guards, that managed the security in that centre. This increased the costs of security severely, forcing the company to limit the costs of security, which can be extremely hazardous to the interests of the enterprise, as the company cannot assure the information is well secured, as well as workers.

Bringing up what was explained in the chapter *Project Origin*, other problems aroused when all the security and the informatics of the company were decentralized, like the case of universality of the access. If an executive from Barcelona travelled to Brazil, his/her access control card would not be recognized by the card reader, because he/she is not a worker of that centre. Consequently, access would be denied, and the executive would have to demand access specifically for that reason. That type of situations could reduce the pace of the projects and would certainly be quite intrusive for the worker, probably offending him/her.

Therefore, the solution that this project proposes is to centralize all the management and control of security at every level, not only the perimeter security, but also and more importantly, the networking.

In order to make that centralization happen, all the perimeter security devices must “speak” the basic communication protocol existing nowadays, TCP/IP, to ensure devices can communicate with the controller, and to be accessible from other networks, such as, for example, the Internet. Also, key services such as Active Directory and basic servers like DNS and DCHP will also be installed in every location to ensure the communication between devices.

The security will be centralized in Barcelona, on a special security room with at least two or three security personnel in charge of the control of the security software that

manages the hardware (perimeter security devices).

As a conclusion, this project will organise both a perimeter security structure and a network structure supporting these devices in order for them to communicate as efficiently as possible.

5.1. Network Structure / Perimeter Security Structure

5.1.1. Network Structure

The investment the company has to take matters into is not just on the need of buying all the necessary perimeter security devices with capacity to communicate using TCP/IP but in order to make this communication viable, a whole new network structure must be assembled.

Until now, *HidroPlastic S.A.* has had a very poor networking administration. All workers had access to almost every server set up in the company: there was absolutely no control of the physical structure of the company, as there was not a system that controlled the number of machines, the number of users, and the user's policies when it came to network access.

Apart from that, communication between devices was not TCP/IP driven, but generally communications were held by means of third-party services, such as mail and post office.

Consequently, there is a need to thoroughly update the networking from the company. This update will include adding:

- Servers
    - DNS
    - DHCP
    - DC
    - File
- Next-gen Firewalls (Application firewalls)

- Back-ups
- Local software security
    - Anti-Virus
    - Local Firewall

The intention is to create a structure similar to this one:

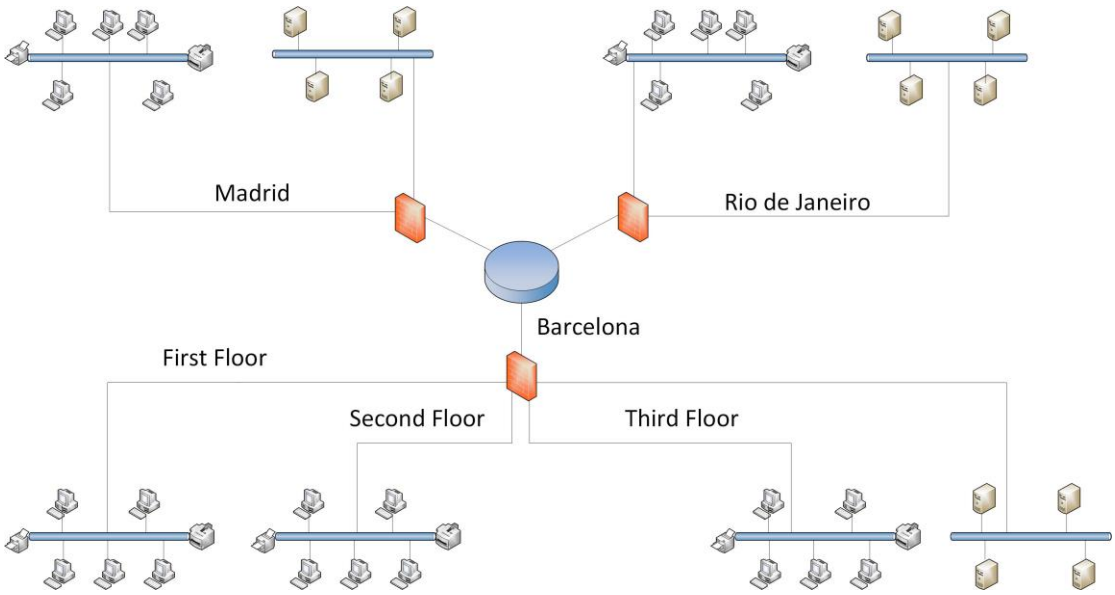

Figure 46. Network Structure.

Legend:

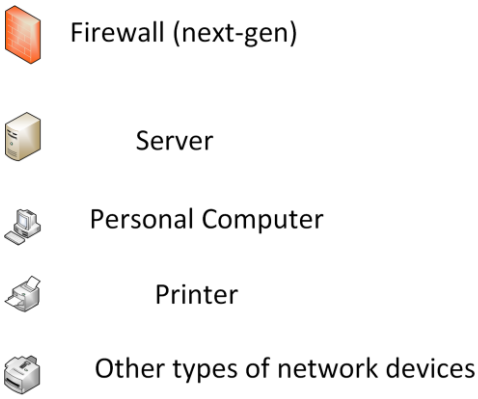

Figure 47. Legend 1

5.1.2. Perimeter Security Structure

Once the network structure is assembled, we shall proceed to integrate the perimeter security structure “on top” of it, to work as properly as planned.

As explained in previous chapters, the intention is to control this perimeter security structure in a centralised manner and to do so we need to install a monitor room (chapter 5.4) from which this security control will be done.

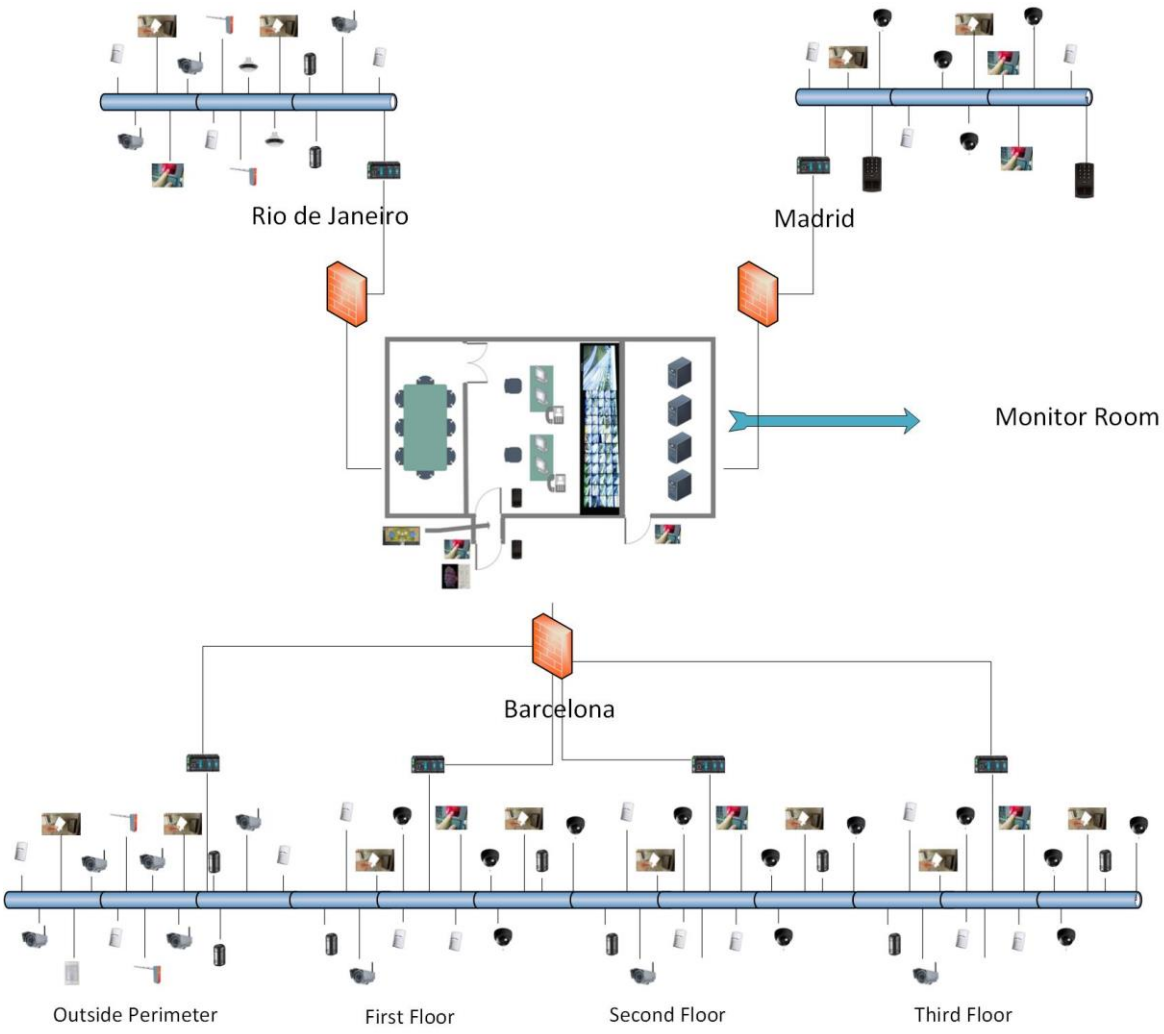

Figure 48. Perimeter Security Structure.

Legend:

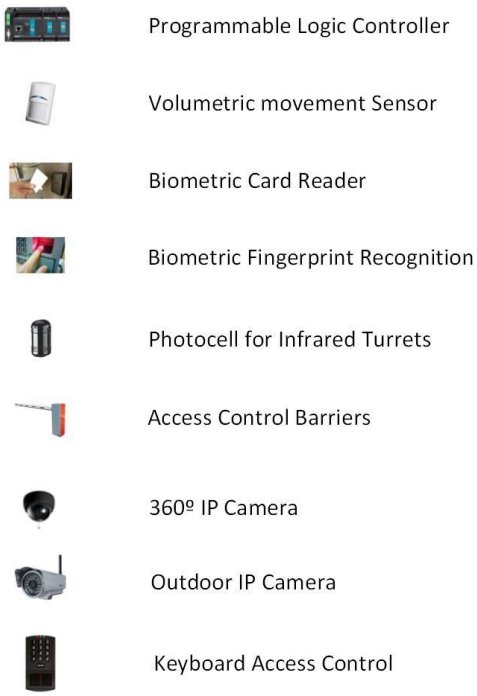

Figure 49. Legend.

5.1.3. Structure Functioning

The main goal of all this investment is to create a system on which all the devices are linked onto the servers to establishing an IP-based communication.

However, all these devices must be connected to different controllers for a reason.

5.2. Server distribution

Apart from the perimeter security, other types of servers have to be organised and distributed. In order to accomplish everything that was demanded, such as the universality of access and the correct communication between security devices, some other servers along with the software they manage have to be assembled. It has to be noted that this server organisation is meant for Windows Servers, not any other type of operating systems. These are:

- Domain Controller Server
- DNS[39] Server

- DHCP[40] Server
- File Server
- Back-up Servers

5.2.1. Domain Controller Server/ Active Directory

This server is in charge of managing the Active Directory, which is a Directory Service[41]. The principal duty this server has is to control security authentication (loggings, password management and user policies). To do so it uses the Active Directory (introduced with Windows 2000).

The basic principle of this service is to store the information of all the computers, groups of users, users and domains[42] the company has, as any other resource you can imagine, as well as their security and access policies for users.

Therefore, what Active Directory gives us is basically the chance to create and control a physical network structure in a logic way.

To represent that network structure, Active Directory uses “objects”. These objects could be servers, users, clients, groups of users, computers etc. Objects represent the smallest type of element inside an Active Directory and, you can have organized units made up of objects, domains, “trees” and finally “forests”. This establishes a hierarchy that will eventually define the structure and permissions in the network.

It is important to note that domains (hidroplastic.local for example) can be divided into subdomains, also known as “child domains”. For example, when the time comes and we create a domain for the Brazilian location, we will create a domain called Brazil.hidroplastic.local). This domain will group all the objects (users, clients etc. from Brazil). This would create what is called a “tree”.

Finally, if we regroup to independent domains (for example the company unites with another company to expand their market) this would be the creation of a “forest”.

The main reason Active Directory has become so extended and used globally is due to the fact that it is a very simple way of centralizing the administration of a represented logical network that emulates the physical one the company has, facilitating the administrators the duty of controlling who has access to what

resource, who has not, where a certain user logs onto which client etc.

Moreover, it is very relevant to emphasize on the administration of the permissions users have. Controlling who has access to certain information is key to protect that information that could be critically important for the company. Denying access to users who should not have access to that information is very important. You can even control at which hours a certain user has access to log in, or not. This object in charge of controlling user's policies and permissions are called GPO (group policy objects).

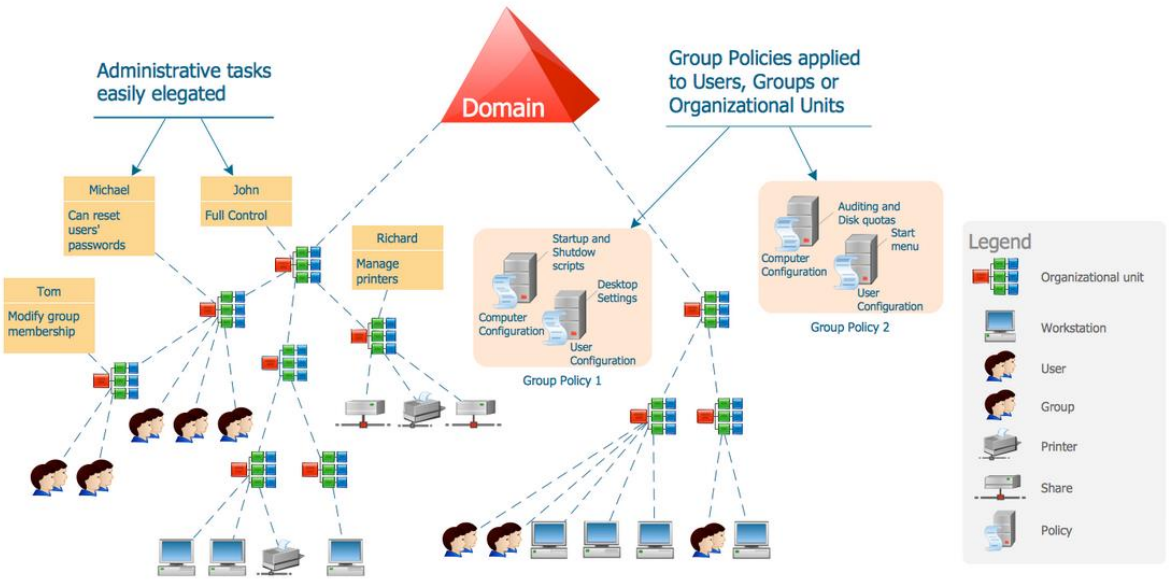

Figure 50. Active Directory. Conceptdraw.com

As we can see in the ilustration above, it stands out how simple a network can be represented. Although this is not Active Directory, it is a very visual way of understanding what Active Directory does.

However, Active Directory is presented another way, in a more than familiar manner, which is by a set of folders.

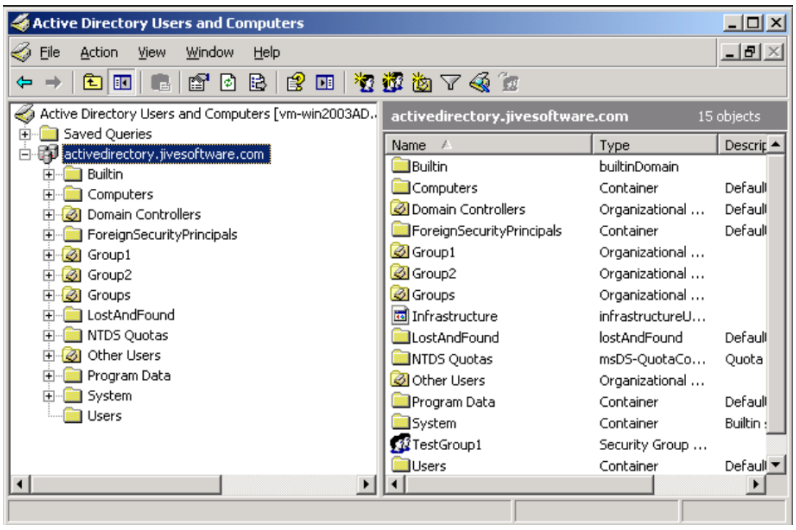

Figure 51. Active Directory.

On the left hand side in *Figure 51.* we can see the different types of folders that Active Directory in particular has, such as Computers, Domain Controllers (servers), groups of users etc.

Conclusively, having Domain Controller Servers (hence, having an Active Directory set up), is more than important for the interests of the company, as the administrators can easily control and manage all the elements in the company in a centralized and comfortable manner, and therefore protecting the information that should not be open to everyone's hands.

5.2.2. DNS Server

DNS Servers play a fundamental role in the organisation of networks nowadays. Everything inside a network has an IP address[43] assigned to them. These addresses are very long, and extremely arduous to memorize. For that reason, the DNS service was created, in order to translate these IP addresses into more simple names, for users to memorise them easier.

When someone types into the computer "www.google.com", they are redirected onto that particular site by writing a very familiar and easy to remember domain name. Once that name is typed onto the web browser, by means of travelling through many routers the browser finally redirects the user into that domain, doing all this in a blink of an eye.

However, all this communication is done by means of IP addresses, not domain names, as these devices communicate using IP addresses. So this is what DNS does. The web browser receives a petition to go to a certain domain name. The browser then looks up in its cache (memory) to see if it that domain name has been researched before. If not, it then demands its specified (in the computer's properties) DNS server what domain is actually (its IP address). If this DNS server does not know what IP address corresponds to that domain name, it asks then the secondary DNS configured to our computer.

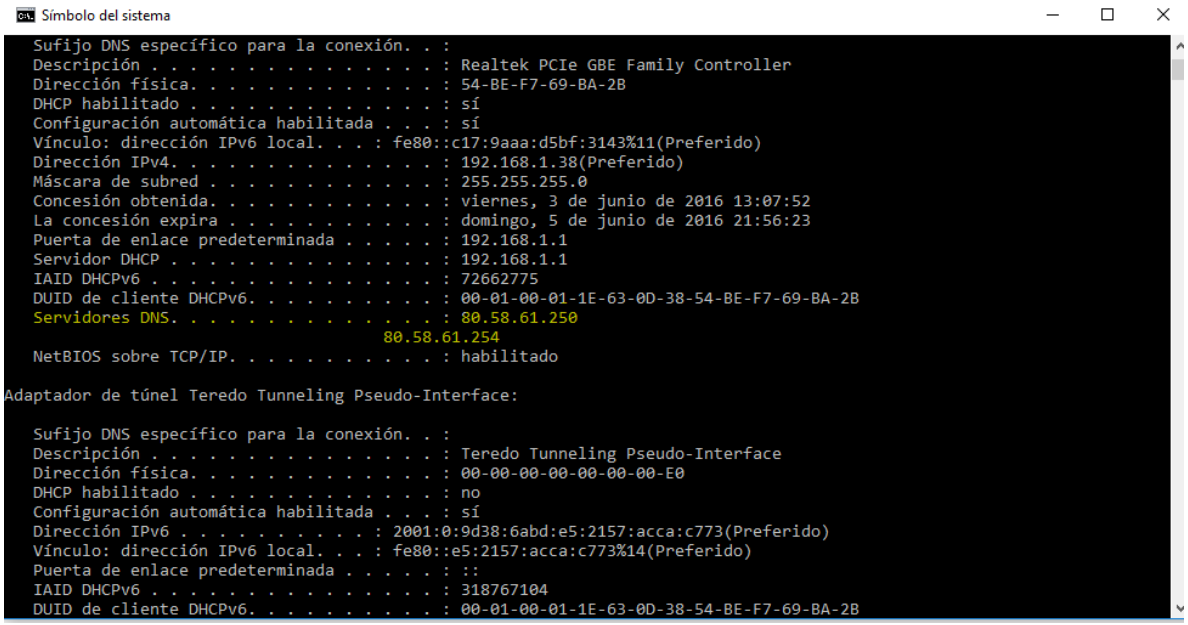

Figure 52. My Computer's Configuration

In the case of my computer, I have these two DNS servers configured (almost all computers do, as it is a save way of assuring you always get the address you want). If that domain name is not stored in the cache, then they will "scale" the petition to other DNS servers, named root name server, TLD name server and authoratative name server, in that order. A very common utilised DNS is Google's, which is 8.8.8.8 or 8.8.4.4.

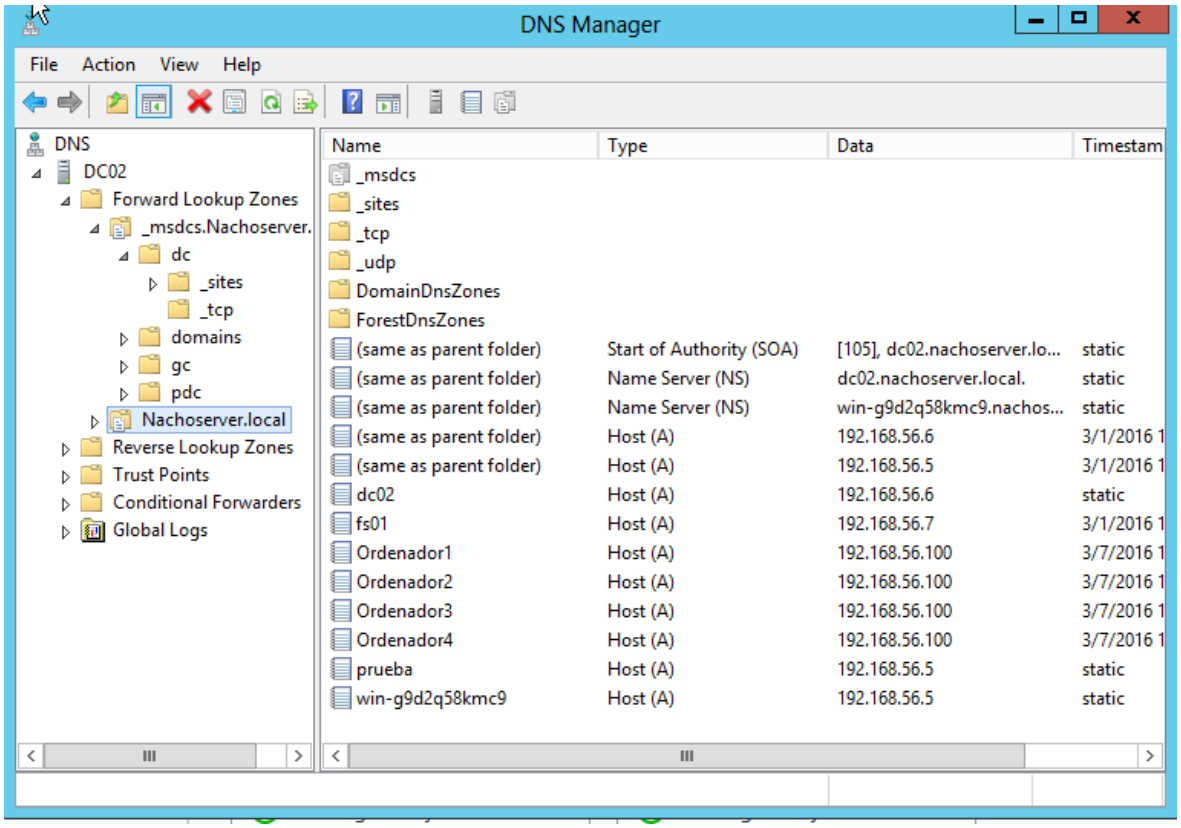

Figure 53. My Personal DNS.

5.2.3. DHCP Server

In order to fully comprehend this type of server, first we need to detach and understand the two types of IP assignments. You can have a fixed IP or a dynamic one.

The vast majority of Internet users do not even know this, but they have a dynamic IP service running in their network. Every time they log onto their router, the router uses the DHCP service to assign an IP to that device as long as it remains connected to the network. Some more advanced computer users will maybe decide to fix their IP in order to have a unique address. In almost every router, it comes with a certain pull (range) of IP address it can assign to the devices that enter its network (previously identifying itself). This range is variable, and you can vary it by entering into the configuration system of the router (typing the router's gateway onto the web browser and typing the administrator's username and password). In this portal you can also vary many other things, such as fixing your IP, changing the router's password, etc.

As a resume, what a DHCP service gives you is the capacity to administrate a network automatically, as the server does it for you. To do so, the server gives concessions. A concession is when a device enters the network and demands an IP. The server then gives that IP for a certain period of time. When the deadline arrives, the server will send a message, offering an extension of that time. If there is no response, or the response is negative, that IP will be free for further use from other devices (or the same one if it re-enters the network again).

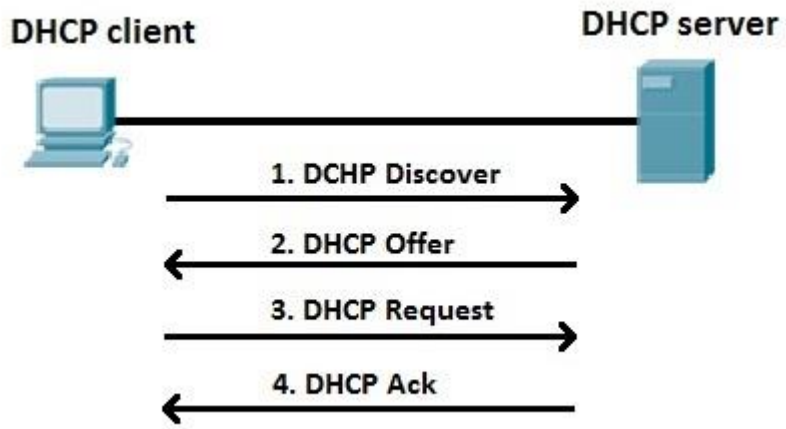

Figure 54. DHCP communication.

On the image above we distinguish the four main elements of client-server communication that occur:

- DCHP Discover: Locates available DHCP servers.
- DCHP Offer: A DCHP server answers that request.
- DHCP Request: IP request from the client. (Other requests may be demanded also).
- DCHP Ack (Acknowledge): Server's answer with several parameters, including the IP address.

Other messages could be:

- DCHP NAK: Concession deadline or the client has a wrong configuration.
- DCHP Decline: The client tells the server that IP is already taken.
- DHCP Release: The client frees the IP address assigned.
- DHCP Inform: The client demands other parameters, as it already has an IP assigned.

5.2.4. File Server

At last but not least, we have the File Server. Probably, the easiest to understand, it basically serves as a database for the information gathered by the company. Its basic functionality is to enable all computers on a network store and therefore, share their files with the rest of the computers by storing them in the network's file server.

5.2.5. Back-ups / RAID

File Servers will be extremely important for one particular reason: They will serve also as *back-ups*. As mentioned on previous chapters, companies are required by law to keep all the information they gather in secondary back-ups, to ensure that if for some reason some important information is lost, it can be easily recovered. The logic to this is that, in case something fraudulent happens in the company, police needs as much proof as possible of all the possible information they might need.

An activity that has become widely spread in companies, especially in big companies is the use of RAID (Redundant Array of Inexpensive Disks). These data storage system that, combining multiple physical disk drives components that distribute and replicate the data, grants the company an increase in integrity, a bigger throughput[44] and capacity. Although RAIDs are a combination of several disk drives, they work as a sole logic unit. This means that the computer in connection with a RAID will only see one disk drive.

5.3. Firewall

Firewalls represent a fundamental part in the protection and administration of the computer security. Basically, a firewall is a software (or hardware) that functions as a kind of “wall” between the computer/server and the Internet (or other networks). It is commonly depicted as a wall in schemes and blueprints. This functionality of this element is that it analyses the information received by internet or by the computer and decides whether this communication must occur or not. As it can control both the computer and the Internet, it is a two-way service.

As a resume, it can permit, block and also redirect different communications between the two sides of the wall. In order to do this, a firewall has a set of rules that have been typed into it that control these permissions. Obviously, some of the rules come by default on the device or software, but others can be written by the administrator of that firewall.

Henceforth, what use could the company give to this service? The answer is many uses. For example, if you want to deny access to certain web sites to your employees, you can type a rule in the firewall, blocking that certain site, like for example pornography, betting web-sites and other type of sites that are not only not acceptable in an office, but could be a source of malware and other type of virus. Also you can establish a hierarchy in terms of permissions. As an example, a rule can be set that if someone logs onto that computer as an ordinary user or as a guest, he/she will have denied access to certain sites that maybe if someone logs as an administrator it will have full access to any website, without restrictions.

Another very important functionality firewalls offer is the possibility to redirect to certain ports. For example, if the user wants to access a web service through the port number 80 (http protocol, which is not encrypted), the administrator could redirect him into another port (443 for example). Another option firewalls have is to redirect to particular websites. If the company as an example only wants to permit access in the Internet to the company’s website, it can write a rule on the firewall for it to redirect all intents to access other web pages onto this one.

5.3.1. Firewalls and OSI model

Briefly explained, the OSI model is a conceptual model that characterizes and standardizes the communication functions of a computing system. It serves as a

visual way to comprehend how communication between network devices occurs, detaching that communication in seven different layers. According to the *IBM Corp*. (International Business Machines Corporation), the model could be shown like this:

OSI Model			
	Data unit	**Layer**	**Function**
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data
		5. Session	Interhost communication, managing sessions between applications
	Segments	4. Transport	Reliable delivery of segments between points on a network.
Media layers	Packet/Datagram	3. Network	Addressing, routing and (not necessarily reliable) delivery of datagrams between points on a network.
	Bit/Frame	2. Data link	A reliable direct point-to-point data connection.
	Bit	1. Physical	A (not necessarily reliable) direct point-to-point data connection.

Figure 55. OSI Model. IBM

This model takes into consideration every part participating in the communication between devices, from the pysical part (the cable which servers as the medium transport) up until the type of application (service) the information uses or works in.

Common, past-generation (they are still vastly used) firewalls usually worked in the fourth layer, the layer instructed to transport. Firewalls basically control this transport and decide whether that communication or transport of information between devices should be accepted. However, this can be hazardous to the interests of a company, as this firewalls are unable to distinguish the type of service the information is using, so no matter what service you use if the firewall does not recognize the port or the communication system, it will reject that communication. This provokes the need to continously update the firewall rules.

Fortunately, a new-generation of Firewalls have appeared, and will be surely used by the company. These Firewalls work in the seventh layer, the application layer. What this means is that these Firewalls are able to recognize not only the service (seventh layer) but also control any other OSI layer.

5.3.2. Next-Gen Firewalls

Only recently this Next-Generation Firewalls have appeared. As a briefly introduced

in the paragraph above, these new Firewalls have developed into a whole new concept that includes last-generation Firewalls and their ability to control communications in the Transport layer[45], but now also they can work in the application layer, being able to acknowledge the type of service used in the communication.

One of the most important services these Firewalls offer are the IDS and IPS:

IDS (Intrusion Detection System): This device or software application that monitors network or system activities for malicious activities or policy violations. The difference between a common Firewall and an IDS is that the Firewall limits the access between networks, they prevent a communication. On the other hand, an IDS assesses whether a communication that has already taken place is suspicious of being fraudulent or dangerous.

IPS (Intrusion Prevention System): Also known as IDPS (Intrusion Detection and Prevention Systems), this network security application monitors network or system's activities in research for malicious activities. The main difference between IPS and IDS is that IPS not only detects the hazardous activity but also takes matters into its own hands and blocks that communication. At hindsight it may seem always a better option than IDS, but at some situations it is not as recommended as this system will block any unknown dangerous communications, even if the company knows that is not a hazardous activity.

What makes the next-gen Firewalls great is that they include one of these services of both, making this Firewall a security service at almost all levels. Adding these applications makes the Firewall a sort of anti-virus at a network level (anti-virus normally work at a local level).

5.3.3. Chosen Firewalls

As shown on the network structure diagram, the company will need three next-gen firewall devices to succeed in its commitment (apart from the local computer firewalls).

For this reason, firewalls play an extremely important role in this project. Henceforth, we need to buy the best product that can be found in the market, and these are the firewalls from *Palo Alto Networks*. *Palo Alto* offers a great manifold of different Firewalls for different levels of throughput (performance), capacity, sessions and

speed.

Consequently, our plan is to install a very powerful Firewall in Barcelona, and two minor ones in Madrid and Rio de Janeiro.

PA-5050 (Barcelona):

- 10 Gbps firewall throughput (App-ID enabled)
- 2.000.000 max sessions
- 120.000 sessions per second
- 125 virtual routers

PA-200 (Madrid and Rio de Janeiro):

- 100 Mbps firewall throughput
- 64.000 max sessions
- 1000 sessions per second

Figure 56. PA-5050 and PA-500. Palo-Alto Networks

5.4. Local device security

So far all the devices explained work at a network level, but each personal device must also have access to their own local security. This security software will consist of a personal Firewall, an anti-virus software and an anti-spam.

- Local Firewall: As well as the network structure Firewalls, the local ones will also be Next-Gen Firewalls.

- Anti-Virus: Software in charge of detecting and eliminating virus that try to enter the device. Traditionally, anti-virus were created to prevent, detect and eliminate viruses. However, with the evolution of the Internet anti-virus's developers have had to adapt to a more global threat, named malware. Malware is any type of malicious software, including not only virus but also trojan horses, worms, ransomware, spyware, adware or scareware.

- Anti-Spam: Method used to prevent junk mail from entering your mail. This junk mail is known as Spam.

5.5. Monitor Room

For a start, we need to study in detail how this room will be. This room, only accessible by certain people, will be located inside the headquarters, Barcelona.

Inside this room, a video wall will be installed, having access to all the company's cameras worldwide. As this video wall is formed by up to ten different independent televisions, the security personnel will be enabled to change to the camera they want, or even change and manage other software that will be explained in the following paragraphs.

Although it may seem not so necessary, one of the televisions must have be connected to satellite TV, especially news channels, in order to be up-to-date to possible emergencies worldwide, especially in Brazil. In cases of emergencies every second counts, and knowing something is going wrong before having to receive an emergency call from the worker in danger could be key in the wellness of that worker. For example, if a huge riot takes over Rio de Janeiro, our employees working there could be in danger. In case they have not noticed by themselves, the

security workers could tell them before it is too late, or in case an emergency call comes in, the company already knows what to do and how to take matters into account.

Figure 57. Video Wall. Youtube.com

Apart from the ten-TV video wall, two security personnel with knowledge of martial arts, as well as fire weapons (in case intruders manage to enter) will also have a two-monitor computer in their desk to manage the video wall and other devices. Similarly, in their desk, the security workers will have access to a worldwide IP phone, with the possibility to communicate with any worker that needs to talk simply by ringing their specified tag number.

It is important to notice that when workers travel abroad on project duties or whatever they need for work, in case of emergency they will always call first the company, even before calling the police. The reasons could be varied, from the fact of the need to express themselves in their native language (maybe they do not speak Brazilian for example), or the fact that the company has a quicker access to

the police in that country, and could increase the speed of action.

Figure 58. IP Phone 7900 Series. Huawei

5.5.1. Security abroad

This monitor room is especially important when it comes to foreign countries, in our case, Brazil. Apart from having several televisions from the video wall controlling the accesses to the Brazilian building, the monitor room takes other matters into account.

Firstly, the company will have self-designed software that controls and updates the level of risk employee's face in Brazil, indicating with a threat scale how in possible danger they are in. This software takes into account many situations and facts, such as the day-to-day the country is in (altercations, crispation due to political reasons, security issues concerning the metropolitan area of Rio de Janeiro, the number of thefts occurring in the perimeter area surrounding the company's building, among others).

Concerning executives in particular, this matter is even more important, as they not only could be an attractive objective for kidnappers, but he/she could perfectly be transporting very important information, almost for sure at a confidential level. In this case no risk is taken, as he/she will be accompanied by security guards, in an armoured car and even with a panic button[46] located in all the seats of the car, as well as in the trunk. Of course, this panic button will be an IP panic button, in order to be possible to send the corresponding alarm to the monitor room. If it were the case that the executives, in order to reduce costs, reject the armoured car or the personal security, their travel could even be banned by the company, in order to

preserve their integrity.

Figure 59. Panic Button. duanekrip.com

In areas inside Spain security is somehow bigger, although in certain zones the protection the worker can need could be as big as in Brazil.

5.5.2. Access Control

Secondly, the monitor room is also in charge to have visual control, as well as registers of everyone who accesses the main buildings or offices. The images, the time and place of the worker are stored in the servers in case of needing them.

This case in particular is very important in Brazil. As I explained in the previous chapter, legislations back in Brazil are far different from Spain. Particularly concerning workers, they are very protective, and even, they are paid in a different way. This is, they are paid not monthly and assuming a 40 hour a week working hours like back in Spain, but they are paid per accomplished hours.

Hence, they must be thoroughly controlled in what access control concerns, to avoid any fraudulent activities, such as people pretending they have work hours they have not. Also, extraordinary pays are very highly remunerated there, so at night or on weekends access control must be very strict (this would be already assured for security reasons already).

What's more, police could ask for confidential information (previously ordered by a judge), so the company is obliged to store all the information gathered, especially by access control systems and IP Cameras.

5.5.3. Servers

Servers are one of the key factors that reduce costs. Instead of having to install and above all, maintain servers in all the facilities and for various reasons, it is much more economic and logic to install a server cluster[47] behind the monitor room. This cluster will store in the servers all the information registered by the perimeter devices, such as any type of event registered by alarms or sensors, personal information related to workers or access control information gathered these past weeks. This server cluster will be located behind the video wall, on a separate room.

In order to enter that room, biometric systems will be installed, more specifically fingerprint recognition, and keyboard access control (password unique and linked to the fingerprint).

These servers will be located in racks, which will be also closed, therefore needing a key to open them. Inside these racks other devices shall be installed, such as, for example, the controllers in charge of managing the perimeter security devices, as well as the switches, also known as relays.

Figure 60. Server Cluster. deskeng.com 1

5.5.4. Alarm event Software

In third place, alarm event software will need also to be installed. Bringing up the information related to controllers, these devices can store events they have detected, but only temporary. For that reason in particular, we need to store that events information in a server.

That information will be gathered by this software, that will control and have up to date all the information related to alarm events in all buildings. The software will consist of a live blueprint of the building, with all the sensors (IP cameras, movement detectors and so) drawn on the blueprint.

Consequently, the software apply a code of colours, varying from green (no alarm going off from that sensor) to red (alarm went off for a reason). Also the software will have direct communication towards the servers in order to store the information as explained.

Figure 61. Alarm software Blueprint.

5.5.5. Emergency Room

Adding up to what the monitor room consists of, behind both security guards that are managing and control the video wall and the software, there will be a meeting room, for emergency cases.

To serve as an example, imagine an important executive gets kidnapped in Brazil on a travel abroad duty. In that case, the president, as well as the security personnel that are strictly linked to that situation, will come down and meet at this table, in order to proceed adequately. This shall be done to improve the communication between the high directors and the security department, in case the president or closely related executives must take their part in the event.

5.5.6. Access control to the monitor room

As it may seem obvious, access to this room must be very restricted, as the

information gathered and control is very confidential. Therefore, only a very small group of people may have full access to the room, and in case people outside this permission group need access and they have justified the reasons properly, they will receive access, but accompanied by fellow workers that have full access and this person will never be let alone inside the room.

Access to the room will be done through a door, but not an ordinary one. Using the highest and ultimate technology, the door will consist of two doors. The first one, a bullet-proof, as well as explosives-proof glass door, will open once the person or people have properly identified themselves by fingerprint recognition, as well as facial recognition in case of special permissions, and consequently typing a unique password to the keyboard. Once this door is open, you get to another door, same type as the one before. Once the people trying to access cross the door, movement detectors under the floor will detect human activity going on and will shut the door they have just crossed. This will leave the people sort of trapped, and in case they fail to identify themselves when accessing the second door, they will remain trapped and an alarm will go off, leaving them no way of escaping the zone. If they manage to identify themselves on the second door they will then gain access to the room. Of course, plenty of IP cameras will be located around the perimeter of the room, as well as two movement detectors.

5.5.7. Chosen facial recognition device

Trusting one of the best facial recognition device companies there is out there, by the name of *Cognitec*, the company will install, as a security device for the monitor room, the *FaceVACS-VideoScan C5* facial recognition device. This device is an IP video camera with built-in face detection and tracking technology.

- Provides high image quality of machine vision cameras while using bandwith and network structures for surveillance cameras
- Performs real-time, gapless face detection/tracking of multiple faces
- Offers integrated camera control for optimized exposure of the face area

Figure 62. FaceVACS- VideoScan C5

5.5.8. Scheme of the Monitor Room

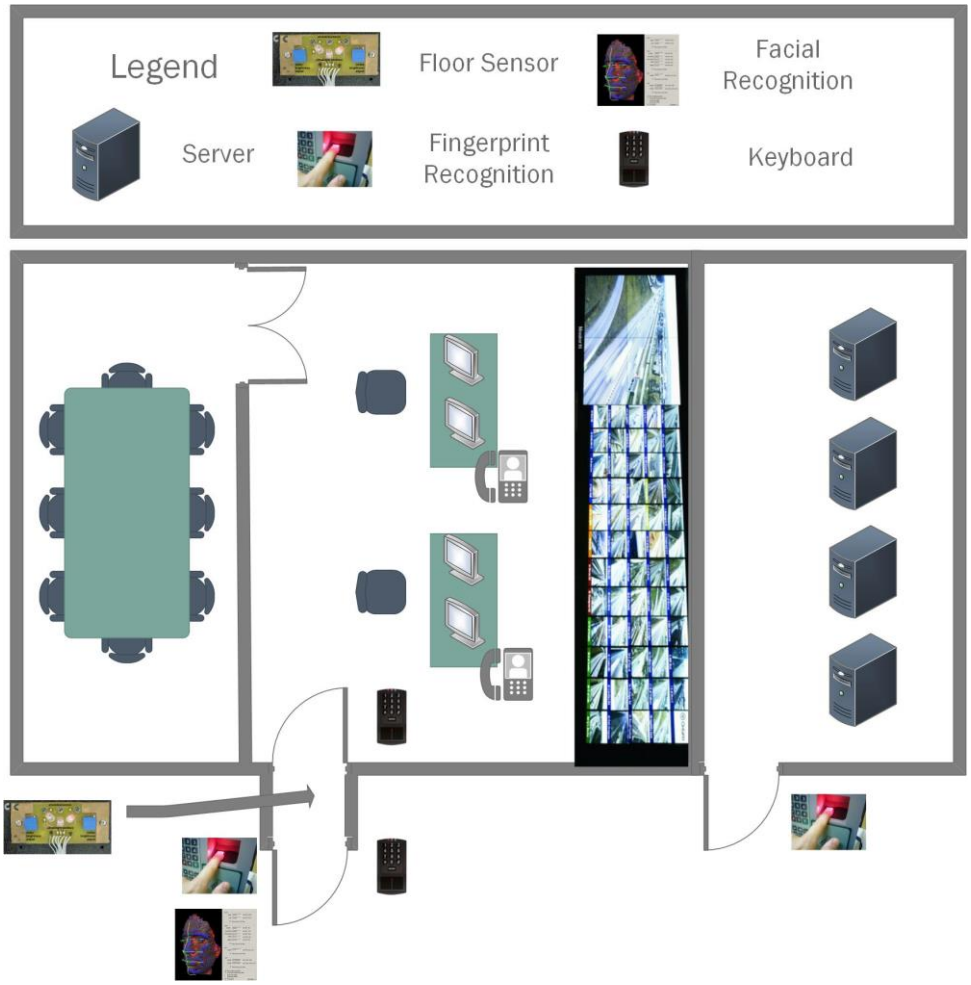

Figure 63. Monitor Room Scheme

5.6. Phases of the Project

In order to ensure the project succeeds, it has to be organised properly, in a logical and sensible manner. Consequently, the project will be organised as follows:

1. Settling the Network Structure
2. Settling the Perimeter Security Structure
3. Integration of both structures

5.6.1. Settling the Network Structure

Firstly, one of the main objectives the company must take into account is that if we have to change all the perimeter devices to change them for another ones, this means that for a certain period of time the company will be almost unprotected against physical attacks. Henceforth, this period of time must be as small as possible. To ensure that, before starting to throw away all the obsolete devices, first we need to install the new network structure from which the security devices will benefit from and communicate with it. By doing this we prevent the company from being defenceless against physical attacks for a long time. Therefore, while the new network structure is being integrated, the old security devices will still be working.

First of all, we need to install the servers. The first server that must be installed is the Domain Controller Server. The reason is that the DC Server holds and manages the Active Directory, which organises all the physical assets (devices and users) of the company. Once the DC Servers are installed, it is recommended to install both DNS and DHCP servers, as both benefit from each other. Apart from that, the DC server uses both protocols in many ways, so all three all complimentary and necessary. Finally, we shall install the File-Servers for both archives and the back-ups.

Once the Servers are installed, the firewalls and the local computer's security must be settled. All devices from the network must be already secured by the time they are integrated into the network, to prevent them from contaminating other devices from the network. Consequently, the local firewall, the antivirus and the anti-spam will then be installed in all devices that need it.

Now that all computers and servers are installed and secured, the network Firewalls

will be next. This network Firewall will be proper hardware, that as the same time they work as Next-Generation Firewalls, they will also serve as routers. Therefore, we reduce costs considerably, as there is a device less in the network. Finally, the switches will be installed in order to manage the devices in the networks such as computers or the perimeter security devices.

5.6.2. Settling the Perimeter Security Structure

As explained in the previous paragraph, we need to ensure that the period of time on which we are changing the old perimeter security devices to the new IP ones lasts as little as possible. Apart from that, it would be a mistake to change all the devices at the same time. Therefore, this change must be done in small paces, and assuring not all the same devices are changed at the same time. For example, it would be a terrible mistake to change all the security cameras at the same time, as therefore the security breach could be very hazardous for the interests of the company, as each new IP Camera must be installed and configured the first time it is placed.

Unlike the case of the network structure, which will be settled at the same time globally, in this case it is preferable to do this installation by locations. As I have thoroughly insisted throughout the last paragraphs, it is critical to reduce the period on which these security devices are installed, so it is a better option to concentrate all efforts (and resources) on one location at a time.Despite the fact all these devices are meant for proper communication using TCP/IP or even UDP protocols using the network structure installed just before, we need to ensure first the devices actually work to deter possible attacks from happening, despite the fact they do not communicate between them.

5.6.3. Integration of both structures

Finally, considering both structures fully installed and operative, it is time to implement them. First of all, all devices will be registered in the Active Directory, along with their permissions (who has the right to configure them). After that, they will receive an IP address by demanding it to the DHCP server. Once this is done, the administration portals of all the devices will be registered in the DNS Servers for further use from the administrators. It will also be necessary to write the consequent communication rules on the firewalls for the devices to be granted the right to communicate. Once all this is done, the integration is finally successful.

5.7. Schemes per location

Using Microsoft Office's Visio 2013, the distribution of the security in each location has been designed, in order to comprehend more visually how it will be distributed.

5.7.1. Barcelona

In the case of Barcelona, the security infrastructure is already built. Barcelona's security system consists of:

- IP Cameras
- Access barriers
- Movement detectors
- Outdoor photocells
- Fingerprint recognition for certain meeting rooms (with keyboard)

In the *Figure 64.* shown below, we can see how the perimeter security will be organised in the presidential floor, where security must be strict.

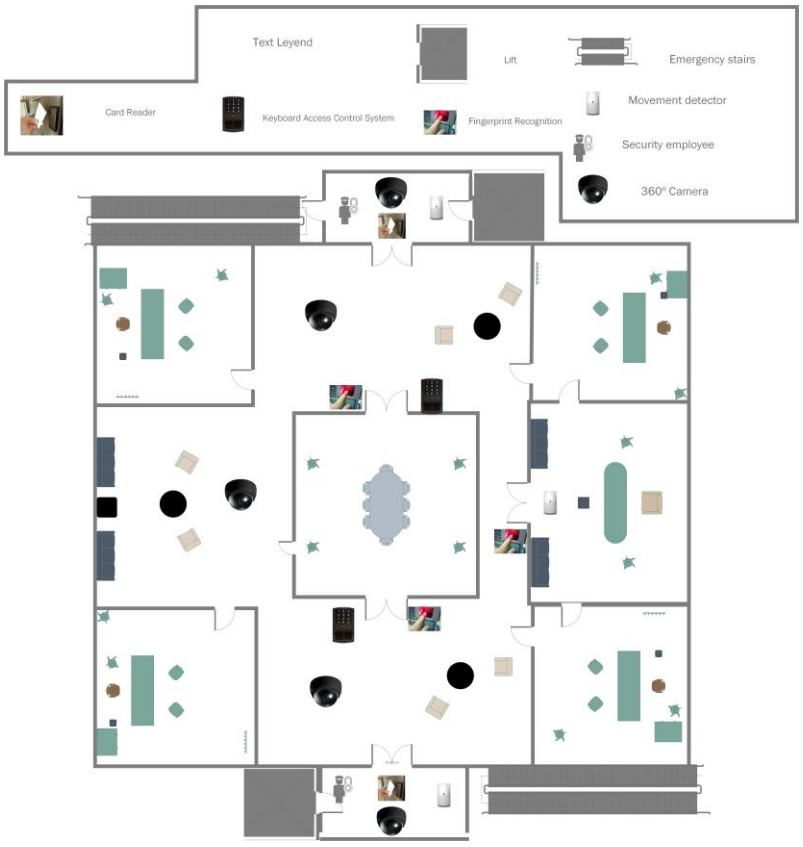

Figure 64. Barcelona floor blueprint. 1

As we can see in the *Figure 64*. above, in the presidential floor everything must be under control. There are:

- Five 360º IP cameras (three in the inside, two in the outside doors).
- Three fingerprint recognition systems (two to enter the main meeting room, one to enter the president's office).
- Movement detectors at the entrance doors of the floor and in the presidential office.
- Security guards at both entrance doors.
- Emergency staircases at both entrances.

The building will consist of three floors. Apart from that, the outdoor perimeter security also had to be assembled.

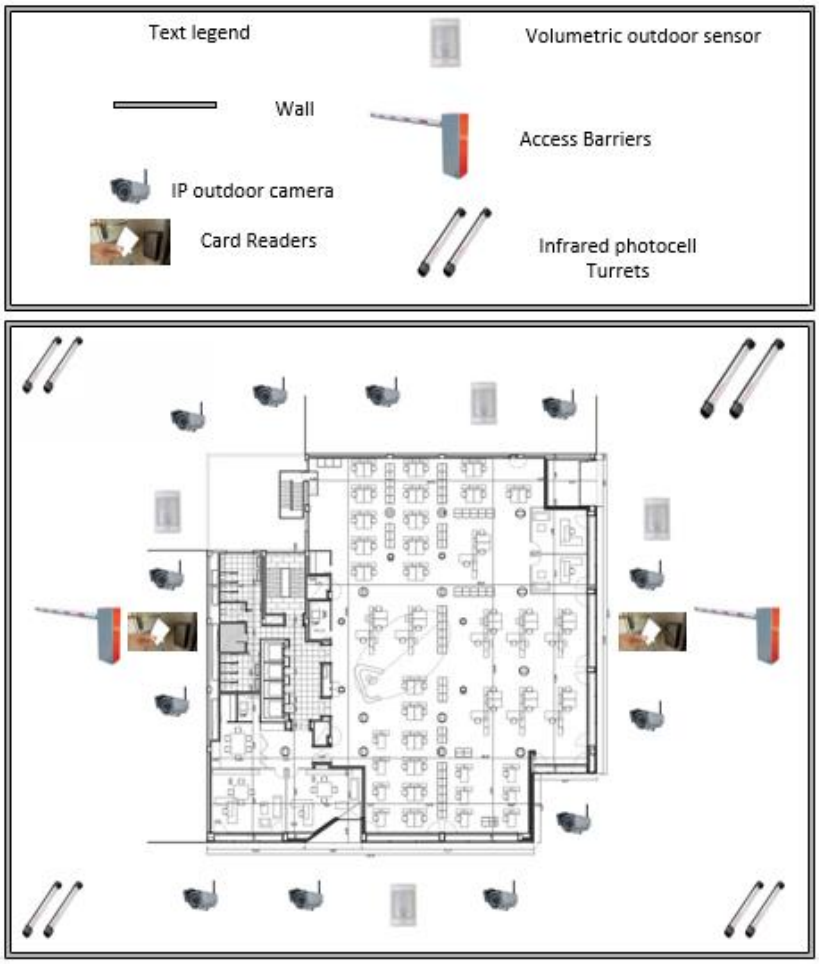

Figure 65. Barcelona Perimeter blueprint

In the *Figure 65*. above the security devices we can see are:

- Four photocell turrets surrounding the perimeter, building an infrared “wall” around the area.
- Four double technology volumetric sensors to notice any undesired movements.
- Twelve outdoor IP Cameras to visually control the entire perimeter.
- Two access barriers one in each entrance to prevent unidentified cars from going in.
- Two card Reader access control systems at the main entrances for employers to validate their access if they have not entered by car (in that case they have to validate themselves in the access control barrier).

5.7.2. Madrid

In the case of Madrid, the company disposes of a single office floor, located in one of the four skyscrapers of the CTBA financial district.

Therefore, most of the perimeter security systems mentioned on previous chapters, such as barriers, outdoor detectors or photocells, cannot be installed here because the company has no right to do so, since the company has the right to install anything it may require as long as it is inside their floor. Outdoor security depends on the proper security the building has. This is the main reason most of the sensitive information will be located in Barcelona and not in Madrid.

The security integrated in Madrid’s office will be something like this:

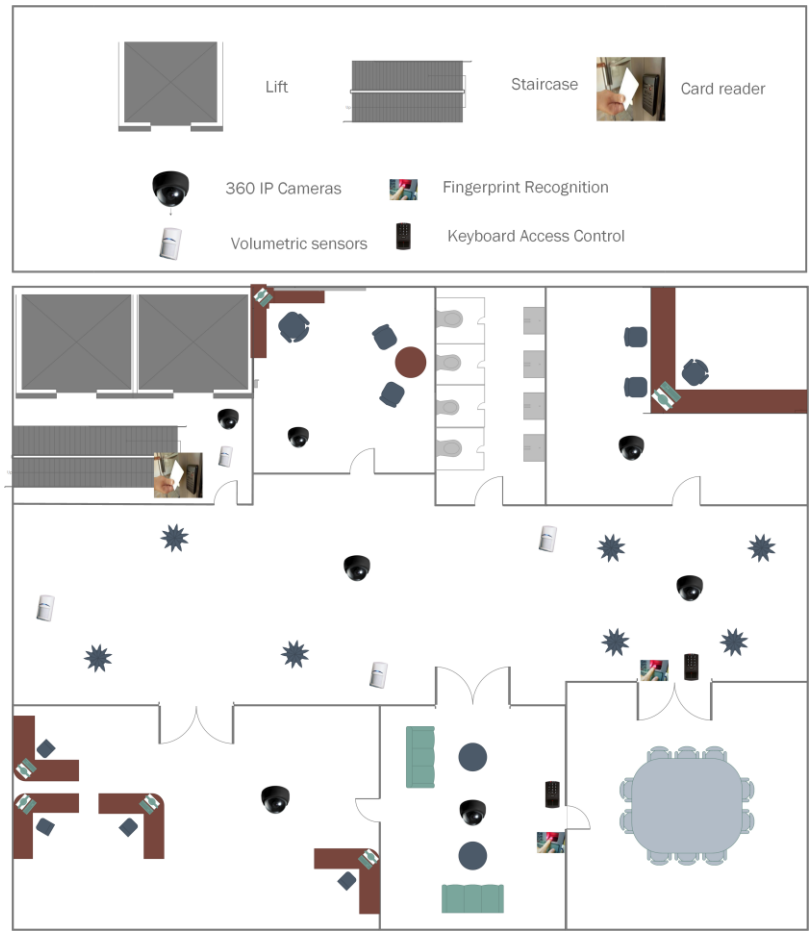

Figure 66. Madrid's Office.

On the image above we can distinguish:

- Seven IP Cameras (in all rooms except on the main meeting room where nothing should be recorded for confidential purposes).
- Four double technology volumetric sensors.
- One card reader access control system to control the entrance to the office.
- Two biometric systems at both entrances of the main meeting room. Both are fingerprint recognition systems and have incorporated a keyboard identification system one the fingerprint is validated, in order to add an extra level of security.

5.7.3. Rio de Janeiro (Brazil)

At last but not least we arrive to the Factory located in Rio de Janeiro, Brazil.

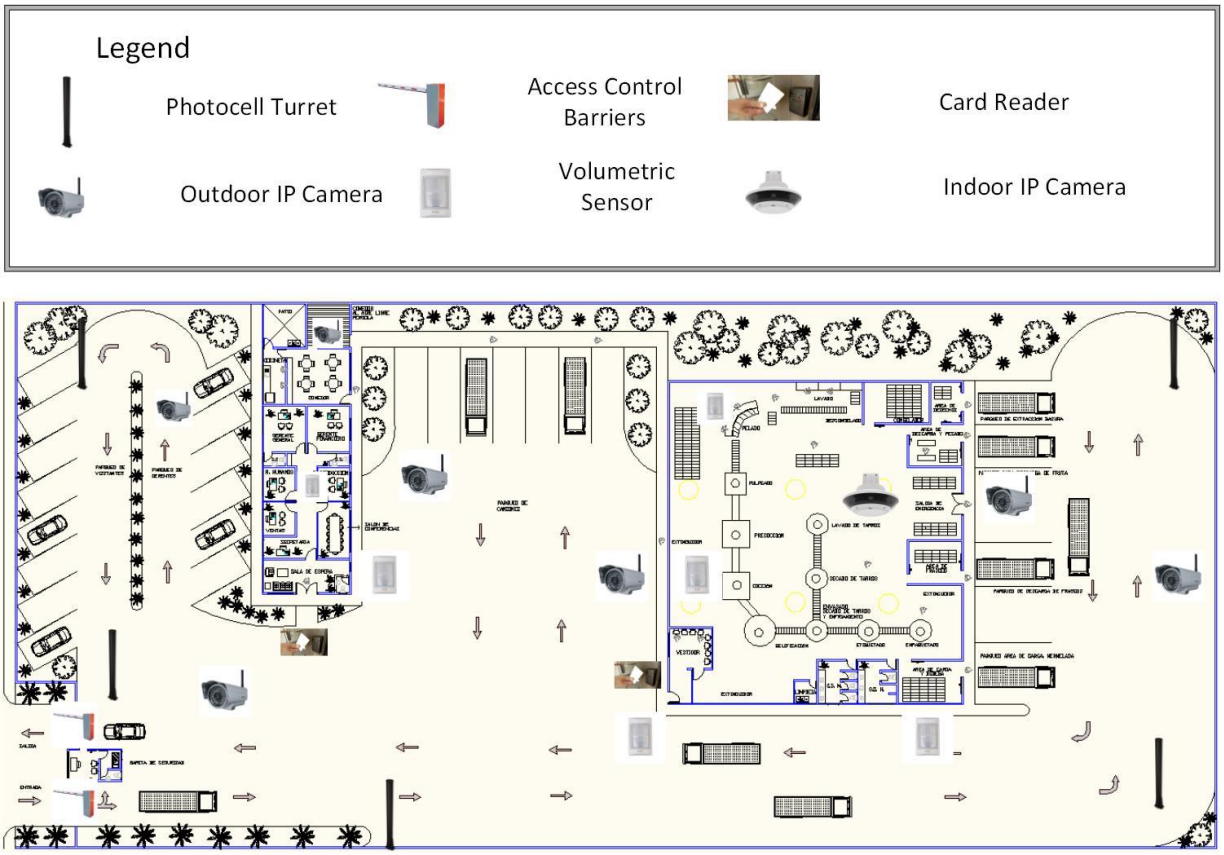

Figure 67. Rio de Janeiro blueprint.

Outdoor Scheme:

- Six outdoor IP Cameras
- Two access control card readers
- Two indoor IP Cameras
- Six double technology movement detectors (volumetric)
- Five photocell turrets
- Two access control barriers

5.8. Budget

The budget is divided into three parts. All prices have been consulted previously with experts.

5.8.1. Network Budget

Network Devices	Price (€/unit)	Nº Units	Total (€)
Servers			0
Barcelona	800	12	9600
Madrid	800	8	6400
Rio de Janeiro	800	8	6400
PA-5000			0
Barcelona	60000	2	120000
Madrid	0	0	0
Rio de Janeiro	0	0	0
PA-200			0
Barcelona	0	0	0
Madrid	2500	2	5000
Rio de Janeiro	2500	2	5000
Video Wall			0
Barcelona	10000	1	10000
Madrid	0	0	0
Rio de Janeiro	0	0	0
IP Phones			0
Barcelona	150	2	300
Madrid	150	0	0
Rio de Janeiro	150	0	0
Security Software	(License)	10000	10000
Batteries			0
Barcelona	1000		0
Madrid	1000		0
Rio de Janeiro	1000		0
MacroLAN			0
Barcelona	1000	2	2000
Madrid	1000	2	2000
Rio de Janeiro	2000	2	4000
			180700

Note: It is important to highlight that international macrolans are more expensive than national ones.

Note 2: We managed to receive a 25% discount from Palo Alto Networks.

5.8.2. Security devices Budget

Security Devices	Price (€/unit)	Nº Units	Total (€)	Security Devices.	Price (€/unit)	Nº Units	Total (€)
IP Cameras (pack)			0	**Barriers**			0
Barcelona	3200	3	9600	Barcelona	2000	2	4000
Madrid	3200	0	0	Madrid	2000	0	0
Rio de Janeiro	3200	1	3200	Rio de Janeiro	2000	2	4000
Outdoor IP Camera (extra)			0	**Proximity readers**			0
Barcelona	200	8	1600	Barcelona	800	8	6400
Madrid	200	0	0	Madrid	800	1	800
Rio de Janeiro	200	10	2000	Rio de Janeiro	800	2	1600
Indoor IP Camera (extra)			0	**Keyboard**			0
Barcelona	100	0	0	Barcelona	150	8	1200
Madrid	100	7	700	Madrid	150	2	300
Rio de Janeiro	100	0	0	Rio de Janeiro	150	0	0
Outdoor Motion Sensors			0	**Fingerprint Recognition**			0
Barcelona	80	5	400	Barcelona	1000	8	8000
Madrid	80	0	0	Madrid	1000	2	2000
Rio de Janeiro	80	4	320	Rio de Janeiro	1000	0	0
Indoor Motion Sensors			0	**Facial Recognition**			0
Barcelona	90	10	900	Barcelona	1500	1	1500
Madrid	90	4	360	Madrid	1500	0	0
Rio de Janeiro	90	4	360	Rio de Janeiro	1500	0	0
Photocells			0	**Photocell Turrets**			0
Barcelona	1500	8	12000	Barcelona	300	8	2400
Madrid	1500	0	0	Madrid	300	0	0
Rio de Janeiro	1500	5	7500	Rio de Janeiro	300	5	1500
PLC			0	**MacroLAN**			0
Barcelona	500	4	2000	Barcelona		2	0
Madrid	500	1	500	Madrid		2	0
Rio de Janeiro	500	1	500	Rio de Janeiro		2	0
			41940				**33700**

5.8.3. Personal Budget

Personal Budget	Price (€/hour)	Hours	Total (€)
Dedicated Hours	40	390	15600
Personal Computer amortization	15	390	5850
			21450

5.8.4. Total Budget

Grand Total	277790	€

5.9. MacroLAN and Internet breakdown/fire

Certainly, one of the first things it may cross the company's executives mind is, what would happen if for any reason, the Internet network breaks down? Will that provoke a security breach as the communications will be shut down? The answer is no.

Consequently, it must be pointed out that the network and perimeter security structures will be unrelated to the Internet network. *Hidroplastic, S.A.* will have their own MacroLAN[48]. This prevents the company from losing the control of the security of the business if for some reason (outdoor casualties uncontrollable by the company) the *Internet* breaks down for a certain period of time.

Therefore, if the *Internet* falls down, the only consequence is that the company won't be able to access *Internet* servers, like any other *Internet* user. The company will hire its own network pull (range) of IP addresses, remaining private and unrelated to the outside networks.

Regarding other hazardous situations that could be a threat to the security, the company has to foresee the chance of an electricity break down. This situations can be common in any building, so the company has to be prepared to confront that situation. To withhold it, the company should invest in special batteries that can sustain the company's electrical needs for around an hour.

Respecting the servers, especially DCHP and DNS servers, the company must invest in extra servers, in case the working ones fall down, because if any of these two servers falls down and there is no substitute, all security devices will lose their IP address

Seemingly, we need to take into account the possibility that our macrolan could break down. In that case all the IP configurations would be disabled, therefore the security devices would be useless. To prevent that we shall install a system mentioned before, which is using controllers as a secondary system to control and utilize the security devices.

The main goal is to control all security devices through IP protocols, but if these fails all the machines will be managed and controlled with the use of controllers, one every sixteen devices, that will be capable of solely controlling all 16 elements and deciding upon instructions.

Although fires are not meant to be studied on this Project as fire sensors are not part of the perimeter security system, they are strictly linked for a special reason. If for any reason a fire sensor goes off, the company is oblied by law and human security policies to open all doors and exits and facilitate the escape as much as possible for all the workers. So in the monitor room the security guard in charge will have a period of ten minutes to decide whether it is a true or false alarm, and if it is proven that a fire has spread, he/she will have the order to open all the doors and exits.

5.10. Antivirus and local firewall

Apart from the security at a network level, the company has to update also the security at a local level, the personal security of each device in the network. To do so, it will use an antivirus and a local firewall.

The antivirus is extremely important, as it will control all the security breaches a computer may have, as normally people using that computers will not use it properly, and maybe their activities could be harmful for the company without them knowing it.

Thereupon, the best enterprise antivirus in the market is the one offered by *Trend Micro*. Its product, named Trend Micro OfficeScan, will grant:

- Protection for file servers, PC, laptops and virtual desktops
- Security against loss and data stealing
- Increase in the throughput
- Process isolation

Concerning the local Firewall, it is included in the proper Windows and its configuration will be subjected to GPO policies from the Active Directory. What this means is that the configuration will be controlled using group policies the administrator will establish in the active directory, affecting to all devices in that group.

Conclusion

Definitely, the results are deeply satisfying. With all this new network and perimeter security arrangement, now all the necessary configurations and the device control are done from one unique point. This resolves in great advantages for the company, as now one or two security workers (inside the monitor room) can manage the whole perimeter security structure. Apart from that, now the universality of access for workers is a reality, as now any worker can travel to another location and get instant access as his/her credentials are recorded by the access control devices that immediately communicate with the DC server which will acknowledge them and consequently the access will be validated. Additionally, with the establishment of all these servers, now the network structure is very well organised, as now all the devices and users are registered in the same place and this enables the administrators to control them with ease.

Over and above, the inclusion of the next-gen Firewalls not only takes the security of the communications to a whole new level, but now they can also route the IP addresses, consequently reducing costs in switches and routers. Now, with the creation of both the perimeter security and network structures, they are fully capable of working as a unison, one controlling that everything is secured and the second one assuring these devices communicate amongst each other and with the programmable logic controllers or servers.

As for the budget, it stayed under what was demanded from the executives of the company, assuring no extras investments must be done. With a top limit of 30000 euros, we managed to stay way under, rounding 278000 euros. This investment is very large anyways, mainly due to the very expensive network equipment. However, it is a long lasting investment, and all these devices, especially Firewalls offer such a huge manifold of advantages to the company that their price will even seem small in the long term.

As a final recommendation it is very important to maintain all the software working in all these devices fully up-to-date, as that could create a very serious security breach.

Bibliography

Bibliographic References

[1] TECNOLOGIA DE LOS PLASTICOS. Polibutadieno. [http://tecnologiadelosplasticos.blogspot.com.es/2011/12/polibutadieno-pb.html , 30th March 2016]

[2] TRABAJO EN BRASIL. Condiciones de la ley laboral en Brasil. [http://trabajoenbrasil.org/condiciones-de-la-ley-laboral-en-brasil/ , 30th March 2016]

[3] DOMODESK. A fondo: Cámaras IP. ¿Qué es una camara IP? [http://www.domodesk.com/a-fondo-camaras-ip , 3rd April 2016]

[4] about en español. ¿Qué es un switch? [http://computadoras.about.com/od/redes/a/que-Es-Un-Switch.htm , 3rd April 2016]

[5] ALLEN-BRADLEY, ROCKWELL AUTOMATION. Presence Sensing Devices. [http://ab.rockwellautomation.com/es/Sensors-Switches/Presence-Sensing , 5th April 2016]

[6] BALLUFF. Contrast (Color Mark) Sensors. How do they work? [http://www.balluff.com/balluff/MMX/es/products/contrast-color-mark-detection.jsp , 6th April 2016]

[7] TWENERGY. ¿Cómo funciona un detector de presencia?. [http://twenergy.com/a/como-funciona-un-detector-de-presencia-912 , 7th April 2016]

[8] SENSORES DE DISTANCIA POR ULTRASONIDOS. [http://www.alcabot.com/alcabot/seminario2006/Trabajos/DiegoPerezDeDiego.pdf , 10th April 2016]

[9] SERVICIOS TC. Volumetric Detectors. [http://serviciostc.com/detectores-volumetricos/ , 10th April 2016]

[10] ACCESOR. Access Control. [http://www.accesor.com/esp/art2_query.php?fam=1 , 11th April 2016]

[11] ACCESOR. Magnetic Band Card Readers. [http://www.accesor.com/esp/art2_query.php?fam=3&sfam=2 , 11th April 2016]

[12] IRIDIAN TECHNOLOGIES. Biometric Comparison Guide. [https://epic.org/privacy/surveillance/spotlight/1005/irid_guide.pdf , 12th April 2016]

[13] IRIS ID. Iris Recognition Technology [http://www.irisid.com/productssolutions/technology-2/irisrecognitiontechnology/ , 19th April 2016]

[14] GOOGLE BOOKS. Advances in Biometric Person Authentication by Stan Z. Li, 5th Conference on Biometric Recognition, December 2004.

[15] BIOMETRIC PB WORKS. Advantages and Disadvantages of biometric technologies. [http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies , 30th April 2016]

[16] BIOMETRIC SECURITY DEVICES. Facial Biometrics An Excellent Time Attendance and Tracking Option. [http://www.biometric-security-devices.com/facial-biometrics.html , 30th April 2016]

[17] BIOMETRIC SOLUTIONS. Fingerprint Recognition and Patterns. [http://www.biometric-solutions.com/solutions/index.php?story=fingerprint_recognition , 5th May 2016]

[18] BIOMETRIC GOV. Hand Geometry. [http://www.biometrics.gov/documents/handgeometry.pdf , 6th May 2016]

[19] BUNKER SEGURIDAD. EPCOM ABT30L / ABT60L / ABT100L [http://www.bunkerseguridad.es/ES_AM/epcom-abt30l-abt60l-abt100l-2-rayos-30m-100m , 6th May 2016]

[20] AGUIRRE NEWMAN. Building blueprint used for the headquarters. [https://www.google.es/search?q=plano+de+edificio+exterior&client=firefox-b-ab&tbm=isch&tbo=u&source=univ&sa=X&ved=0ahUKEwjHgrrz6vnMAhUF1xoKHYF-BjIQsAQIHA&biw=1025&bih=476#imgrc=oG00iUULLKv8RM%3A , 8th May 2016]

[21] EXPRESARTEC. Building blueprint for Rio de Janeiro's Factory. [https://www.google.es/search?q=planos+de+fabrica&client=firefox-b-ab&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjUnoqFjYHNAhWBlxoKHTqDBH

8Q_AUIBygB&biw=1025&bih=476#imgrc=gdRWsxmqFeraJM%3A , 9th May 2016]

[22] Introduction to programmable logic controllers and writing. [https://www.youtube.com/watch?v=ObYwsUhr3Y0 , 9th May 2016]

[23] ACCESOR. DS216, controller for alarm & building management applications. [http://www.accesor.com/esp/docs/DS216.pdf , 3th June 2016]

[24] CCM. El protocol DHCP y su Definición. [http://es.ccm.net/contents/261-el-protocolo-dhcp , 4th June 2016]

[25] IBM Knowledge Center. OSI Model. [http://www.ibm.com/support/knowledgecenter/SSCVHB_1.1.0/glossary/npi_osi_model.html , 9th June 2016]

[26] VOIP SUPPLY. Vivotek IP8335H. [http://www.voipsupply.com/vivotek-ip8335h , 16th June 2016]

[27] VOIP SUPPLY. Basic Vivotek Bundle. [http://www.voipsupply.com/basic-vivotek-bundle#description , 16th June 2016]